



AWS のネットワークで 知っておくべき10のこと

一歩進んで

アマゾン ウェブ サービス ジャパン株式会社
プリンシパル ソリューション アーキテクト
荒木 靖宏
2020年8月19日

荒木靖宏 です。どうぞよろしく

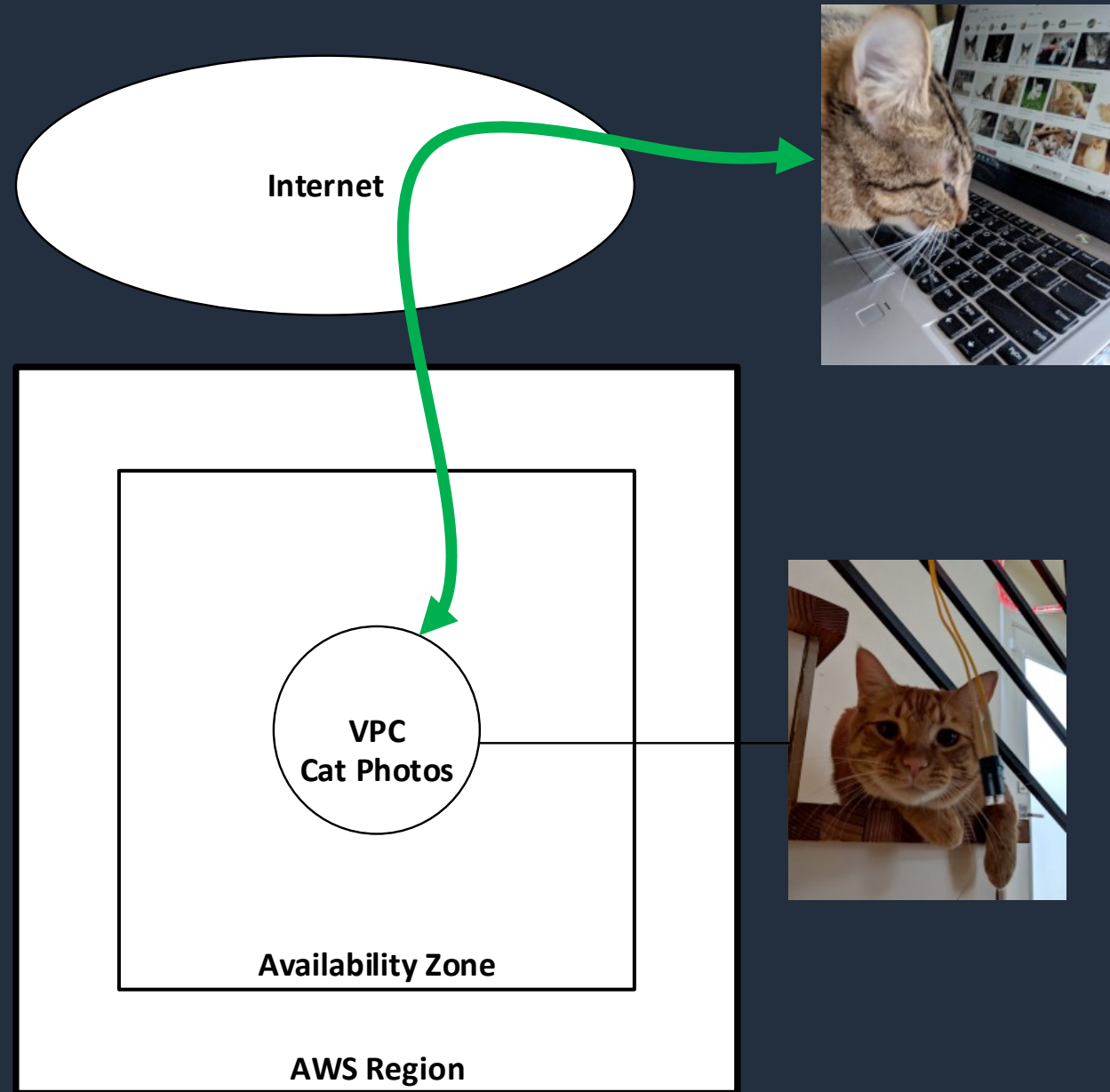
アマゾン ウェブ サービス ジャパン
技術統括本部 ISV/SaaSビジネス本部
シニアマネージャ
プリンシパルソリューションアーキテクト





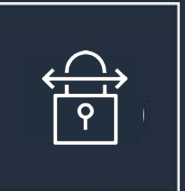
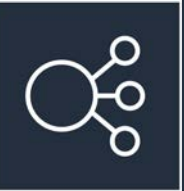








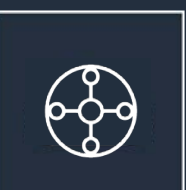










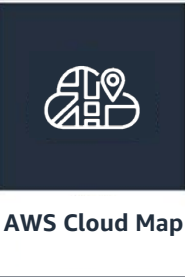
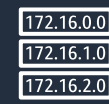







2011年からAWSのソリューションアーキテクトです

人生を変えたAWSサービスはEC2 Spot Instances

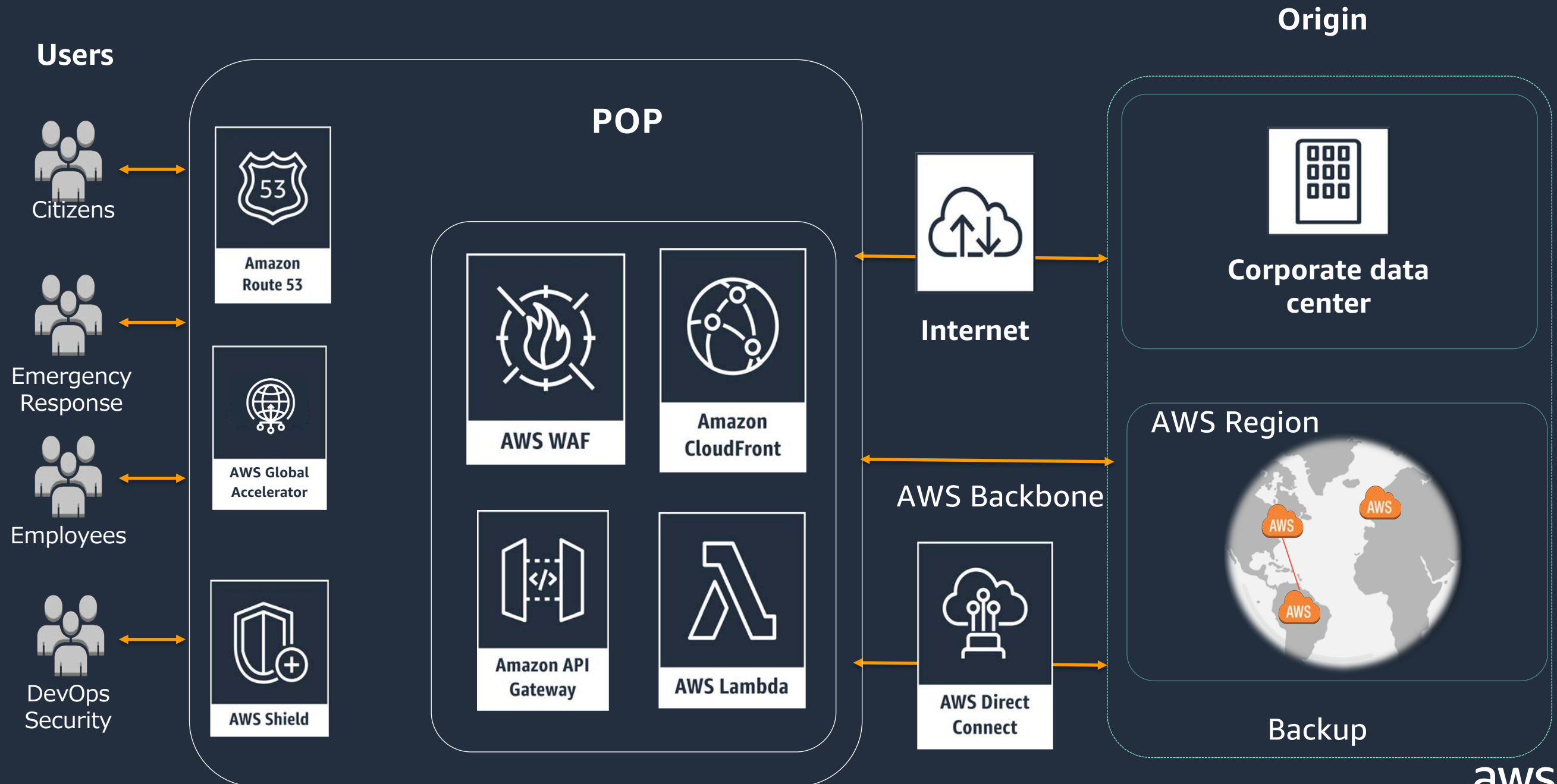
AWSを使う上での漠然とした理解（使用前）



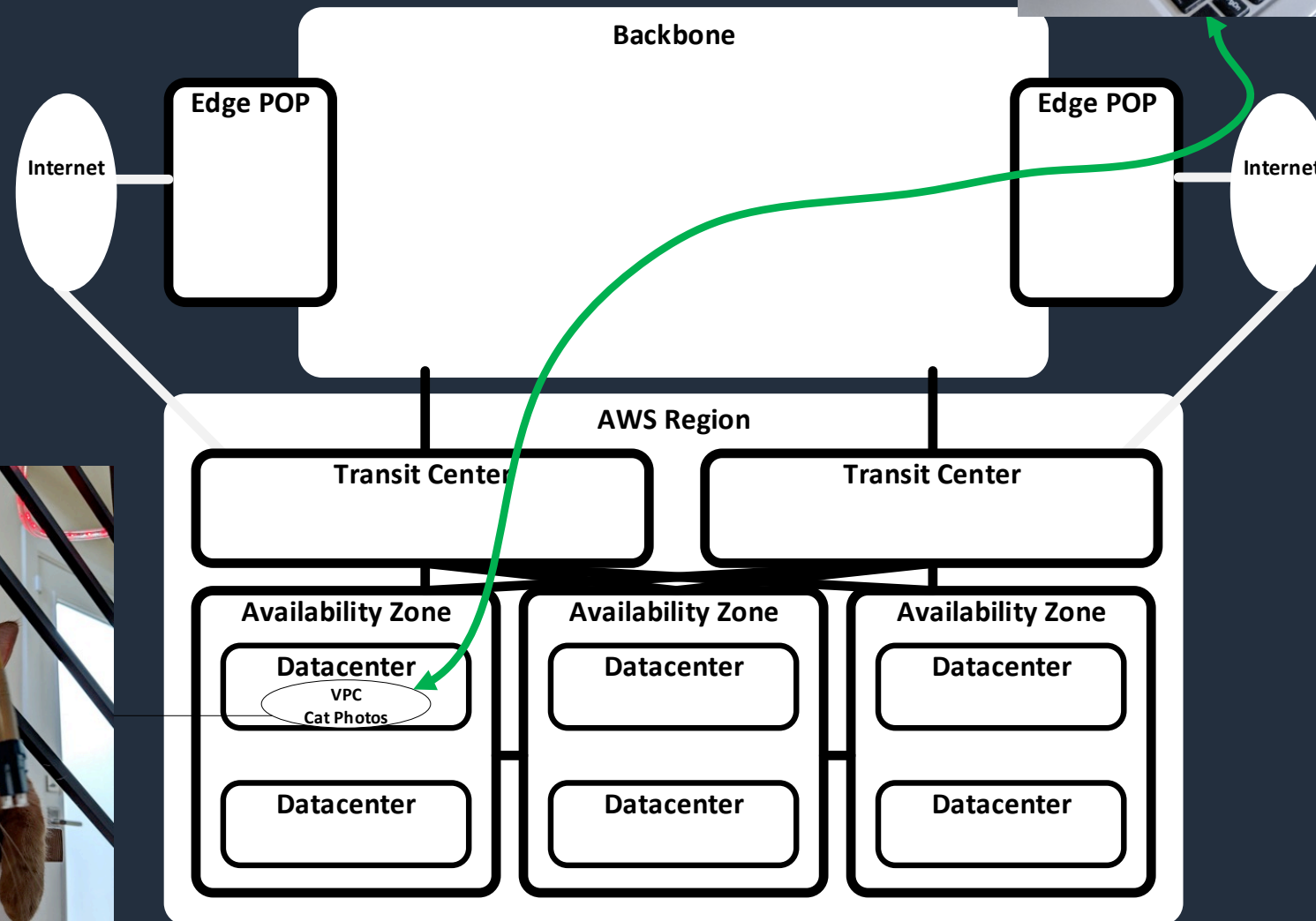
AWSのネットワーク関連サービス群

 Amazon VPC	 AWS PrivateLink	 AWS Virtual Private Network	 Elastic Load Balancing	 Amazon API Gateway	 Amazon CloudFront	 AWS Global Accelerator	 Amazon Route 53	 AWS Direct Connect
 Customer gateway	 ENA	 Elastic network interface	 AWS Transit Gateway	 Site-to-Site VPN	 Application load balancer	 Download distribution	 Hosted zone	
 Flow logs	 Internet gateway	 NAT gateway	 Client VPN	 Classic load balancer	 Edge location	 AWS Cloud Map	 Route table	
 Peering	 Network access control list	 VPC Sharing	 Network load balancer	 Streaming distribution	 Amazon Route 53 Resolver			
	 Endpoints							

Edgeサービス群



このように変われば幸いです（使用後）



アジェンダ

- 本セッションの目的
- AWSのネットワークで一歩進んで知っておくべき10のこと
 1. インスタンス起動からログインまで
 2. インスタンスだけから見える専用ネットワークをつかって情報取得
 3. Amazon Virtual Private Cloud (VPC)
 4. インターネットにつながったクライアントからサーバへの旅
 5. リージョンとインターネットのはざままで
 6. AWSリージョンとグローバルバックボーン
 7. VPC同士を接続する(VPC Peering, Transit Gateway, PrivateLink)
 8. VPCとオンプレミスをつなぐ(VPNとDirect Connect)
 9. インターネットからの攻撃とその対処
 10. ハンズオン&ワークショップで復習
- まとめ

本セッションの目的

対象者

- AWS利用にあたって、ネットワークに関する玄人への入り口を知りたい方

目的

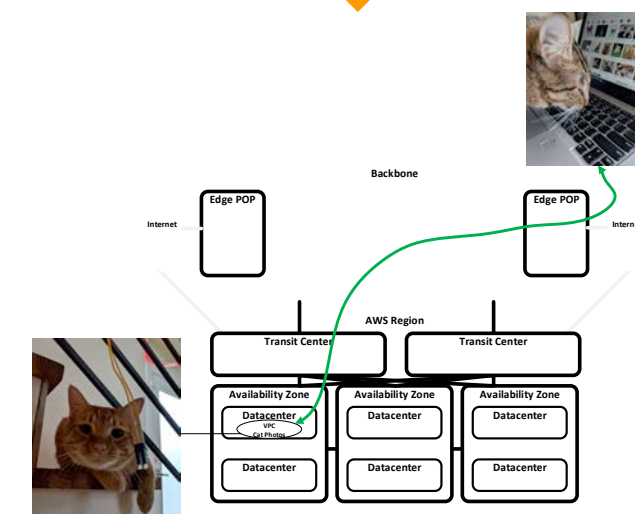
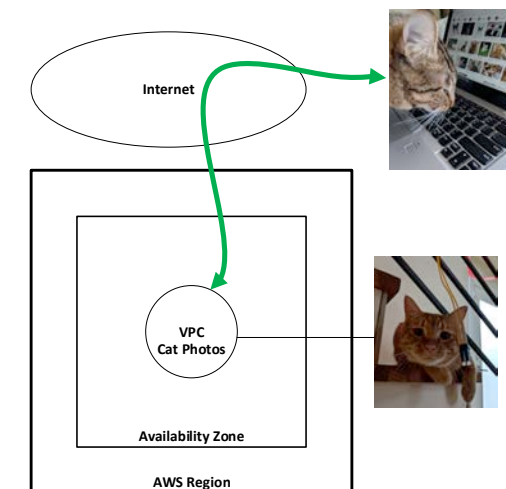
- AWSのネットワークにまつわるネタを話せるようになる
- AWSのネットワークを動かすために知っておくべきことを理解する

AWSを使ったことがない、使い始めたばかりの方へ

AWSを含むクラウドコンピューティングはクラウドというくらいで手元にはリソースはありません。そのため、利用には必ずネットワークを使用します。

したがって、ネットワークの一定の知識は必要です。

ただし、このセッションでは大いにはみ出した内容を含みます。



1. インスタンス起動から ログインまで

AWSのネットワークで一歩進んで知っておくべき10のこと

1. インスタンス起動からログインまで
2. インスタンスだけから見える専用ネットワークをつかって情報取得
3. Amazon Virtual Private Cloud (VPC)
4. インターネットにつながったクライアントからサーバへの旅
5. リージョンとインターネットのはざまで
6. AWSリージョンとグローバルバックボーン
7. VPC同士を接続する(VPC Peering, Transit Gateway, PrivateLink)
8. VPCとオンプレミスをつなぐ(VPNとDirect Connect)
9. インターネットからの攻撃とその対処
10. ハンズオン&ワークショップで復習

2006年8月25日にベータ提供開始

AWS News Blog

https://aws.amazon.com/jp/blogs/aws/amazon_ec2_beta/

Amazon EC2 Beta

by Jeff Barr | on 25 AUG 2006 | [Permalink](#) | [Share](#)

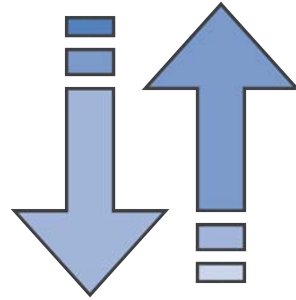
Innovation never takes a break, and neither do I. From the steaming hot beaches of Cabo San Lucas I would like to tell you about the Amazon Elastic Compute Cloud, or Amazon EC2, now open for limited beta testing, with more beta slots to open soon.

Amazon EC2 gives you access to a virtual computing environment. Your applications run on a “virtual CPU”, the equivalent of a 1.7 GHz Xeon processor, 1.75 GB of RAM, 160 GB of local disk and 250 Mb/second of network bandwidth. You pay just 10 cents per clock hour (billed to your Amazon Web Services account), and you can get as many virtual CPUs as you need. You can learn more on the [EC2 Detail Page](#). We built Amazon EC2 using a virtual machine monitor by the name of [Xen](#).

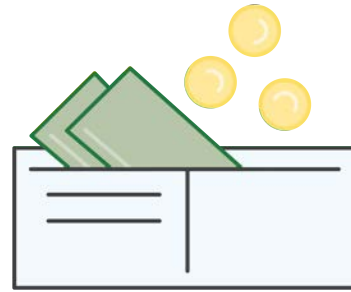
Amazon EC2 works in terms of AMIs, or Amazon Machine Images. Each AMI is a pre-configured boot disk — just a packaged-up operating system stored as an [Amazon S3](#) object. There are web service calls to create images, and to assign them to virtual CPUs to run your application. If your application consists of the usual web server, business logic, and database tiers, you can build distinct AMIs for each tier, and then spawn one or more instances of each type based on the load.



Amazon EC2の2006年当時のコンセプト



必要な時に
必要な数だけ
インスタンスを
APIで起動



従量課金



インスタンスサイズ

m1.smallのみ

- 1 vCPU (1.7GHz Xeonプロセッサ相当)
- 1.7GBメモリ
- 160GBインスタンスストア
- 250Mbps ネットワーク
- \$0.10/hour

EC2発表当時(2006年)と現在の比較

現在と同じ

- 従量課金
- オンデマンド
- API操作
- AMI, Security Group, KeyPairs
- Xenベースの(準)仮想化
- Instance Metadata
- User Data

当時無かったもの

- 秒課金、リザーブド、スポット
- マネジメントコンソール
- 多数のインスタンスタイプ
- 商用OS AMI
- HVM,ベアメタル,Nitro
- VPC, EIP
- EBS
- マルチリージョン/マルチAZ
- etc....

起動時のインスタンスにおけるIPアドレス関連処理

1. DHCPでサブネットのIPv4アドレスからプライベートアドレスが割当（インスタンス終了まで維持）
2. 内部DNSホスト名が割当
3. パブリックIPアドレスの割当（サブネットで有効な場合。EC2起動時に上書き可能）
4. 外部DNSホスト名が割当。プライベートIPアドレスとのマッピングがされる。
5. Elastic IPアドレスを関連付け

DNSサーバーとしてRoute 53 Resolverが動作（DHCPで配布される）

2. インスタンスだけから見える専用ネットワークをつかって情報取得

AWSのネットワークで一步進んで知っておくべき10のこと

1. インスタンス起動からログインまで
2. インスタンスだけから見える専用ネットワークをつかって情報取得
3. Amazon Virtual Private Cloud (VPC)
4. インターネットにつながったクライアントからサーバへの旅
5. リージョンとインターネットのはざまで
6. AWSリージョンとグローバルバックボーン
7. VPC同士を接続する(VPC Peering, Transit Gateway, PrivateLink)
8. VPCとオンプレミスをつなぐ(VPNとDirect Connect)
9. インターネットからの攻撃とその対処
10. ハンズオン&ワークショップで復習

http://169.254.169.254/latest/meta-data/

使用例

- `http://169.254.169.254/latest/meta-data/public-ipv4` でパブリックIPアドレスを知る
- `http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key` からホストのSSH公開鍵を入手。
~ec2-user/.ssh/authorized_keysに書き込み
- `http://169.254.169.254/latest/user-data` に起動時実行スクリプトを置く

実行中のインスタンスからのみ取得可能で、AWS CLIのようなCredential不要

コマンドもあり

- `ec2-metadata`(AmazonLinux標準)
- `ec2metadata`
 - Ubuntu: `cloud-guest-utils`
 - CentOS: `cloud-utils`

169.254.169.254への経路

EC2-Classicでは、169.254.169.254だけへの経路がある

```
[ec2-user@ip-10-120-232-166 ~]$ netstat -rn
Kernel IP routing table
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
0.0.0.0          10.120.232.1    0.0.0.0         UG      0  0        0 eth0
10.120.232.0     0.0.0.0         255.255.255.0   U        0  0        0 eth0
169.254.169.254 0.0.0.0         255.255.255.255 UH      0  0        0 eth0
[ec2-user@ip-10-120-232-166 ~]$ 44
```

VPC

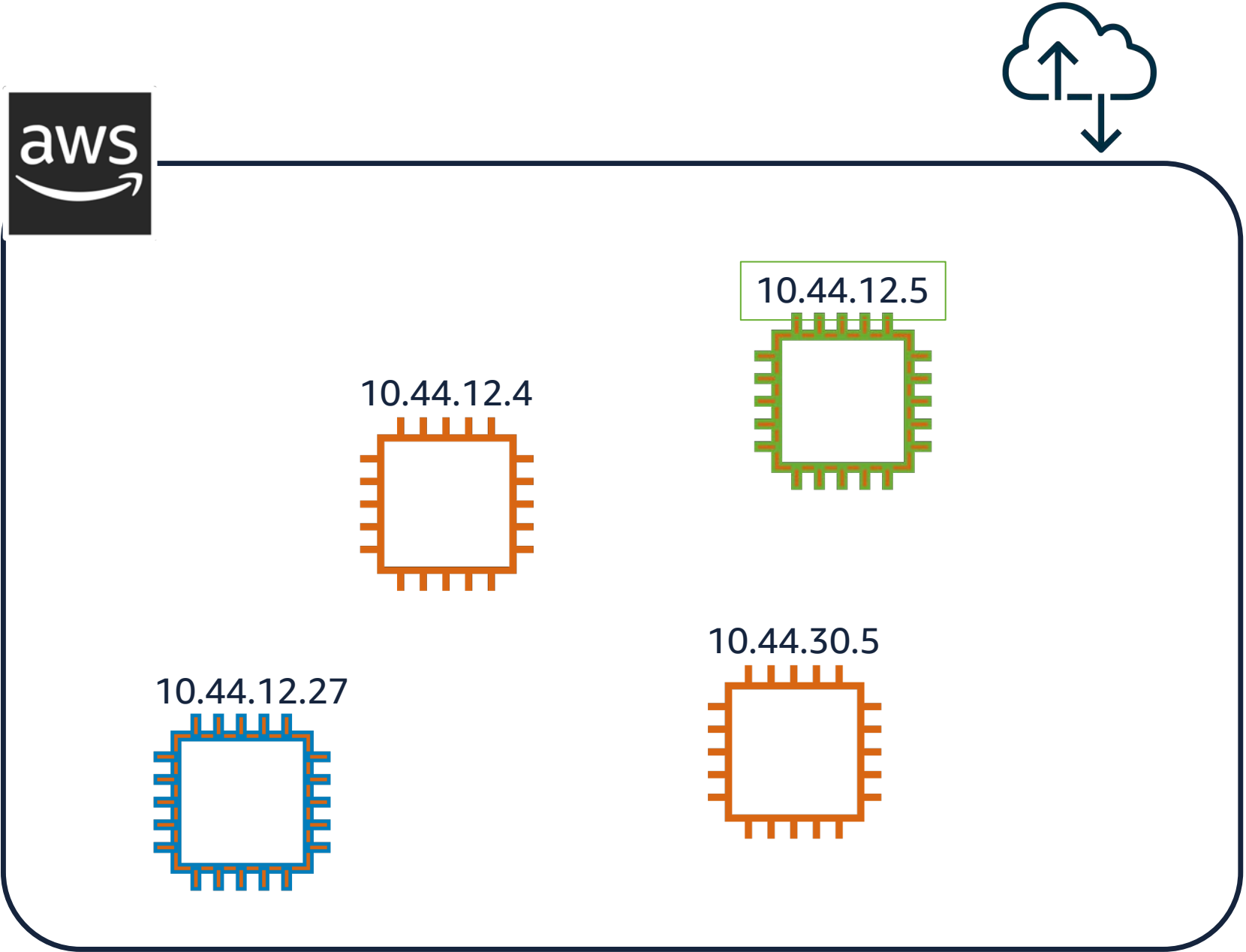
```
ubuntu@ip-172-30-0-214:~$ netstat -rn
Kernel IP routing table
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
0.0.0.0          172.30.0.1      0.0.0.0         UG      0  0        0 eth0
172.30.0.0       0.0.0.0         255.255.255.0   U        0  0        0 eth0
```

3. Amazon Virtual Private Cloud (VPC)

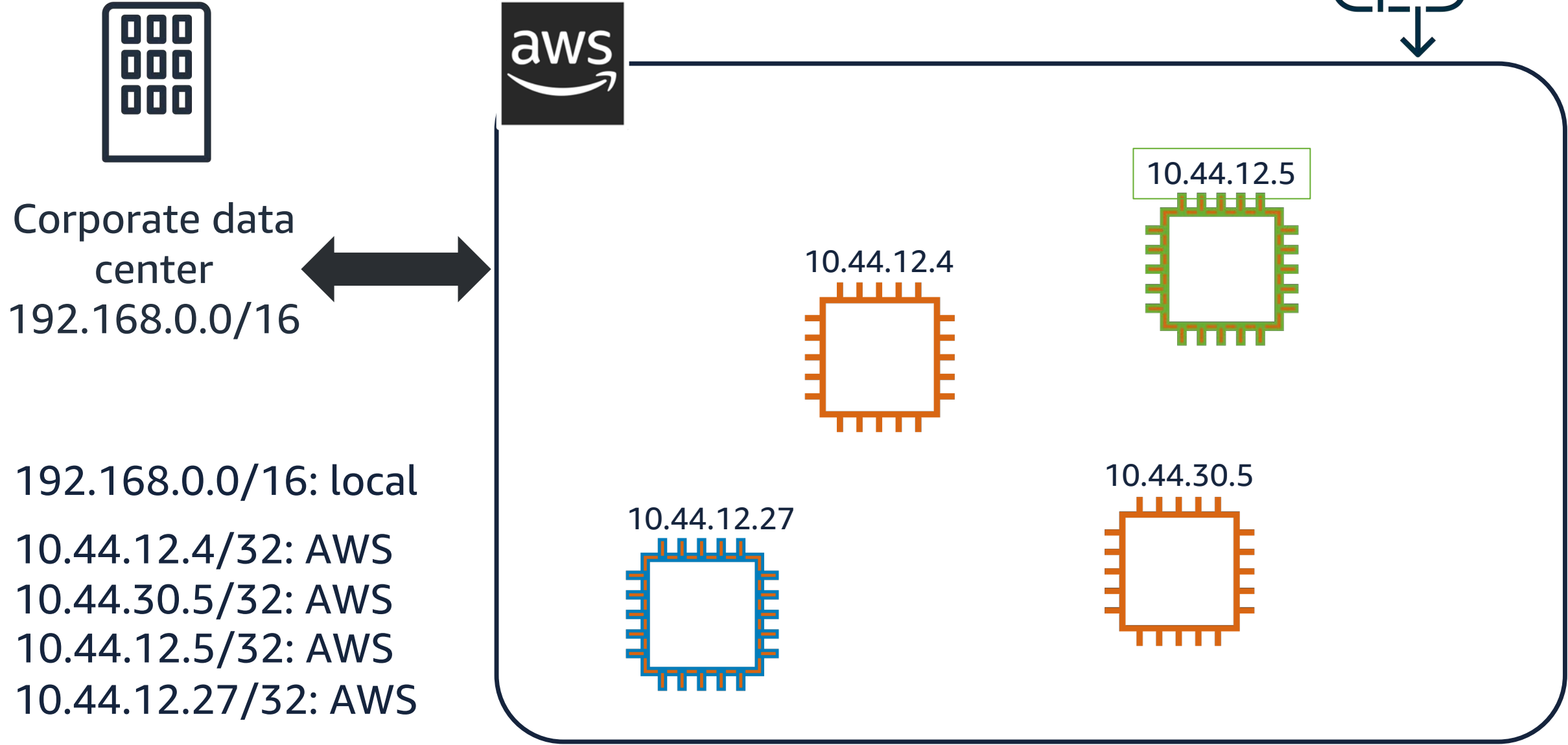
AWSのネットワークで一歩進んで知っておくべき10のこと

1. インスタンス起動からログインまで
2. インスタンスだけから見える専用ネットワークをつかって情報取得
3. Amazon Virtual Private Cloud (VPC)
4. インターネットにつながったクライアントからサーバへの旅
5. リージョンとインターネットのはざまで
6. AWSリージョンとグローバルバックボーン
7. VPC同士を接続する(VPC Peering, Transit Gateway, PrivateLink)
8. VPCとオンプレミスをつなぐ(VPNとDirect Connect)
9. インターネットからの攻撃とその対処
10. ハンズオン&ワークショップで復習

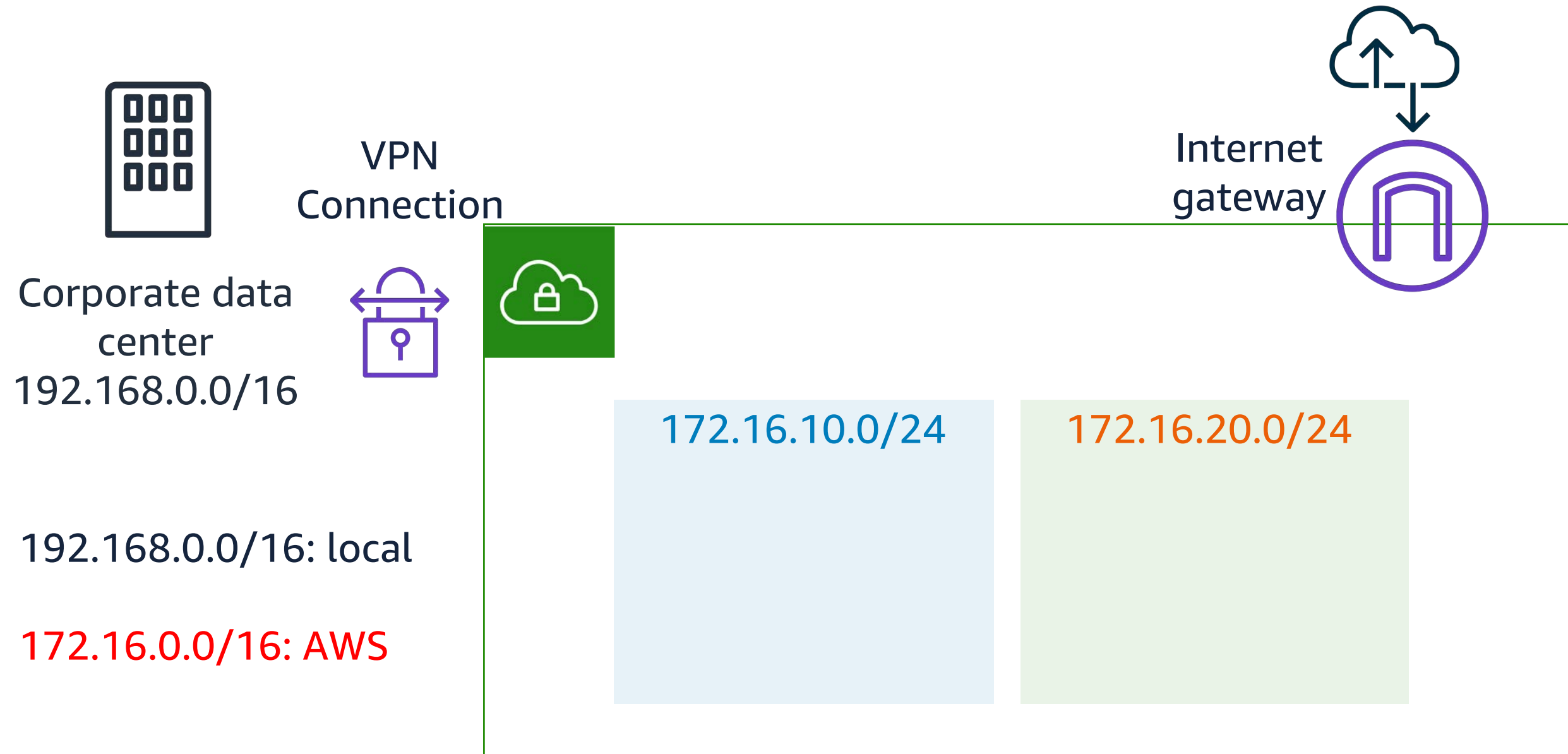
EC2 Classic



EC2 Classicの限界

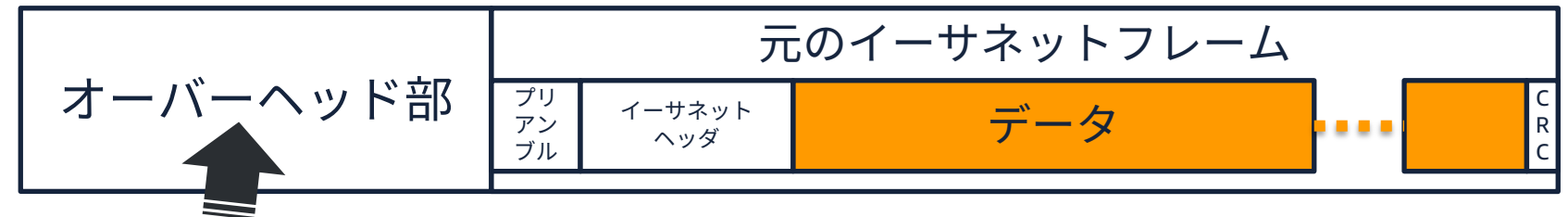
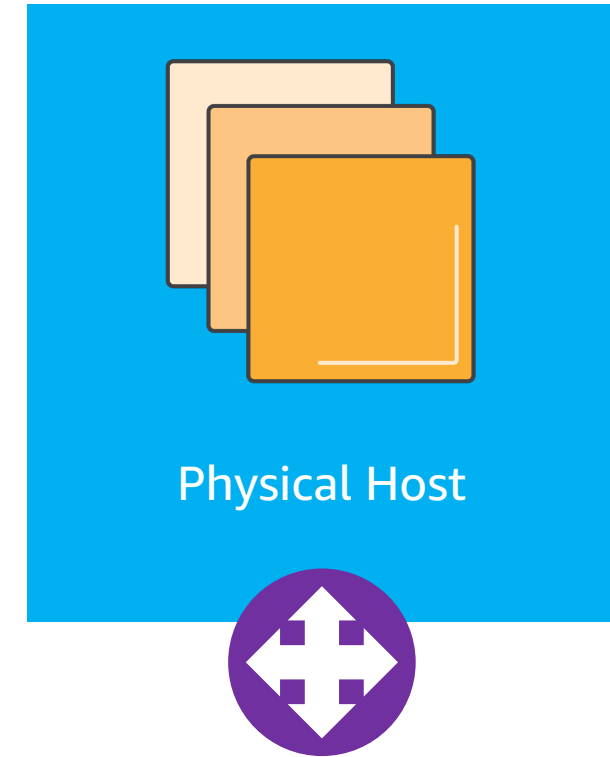


Virtual Private Cloudの登場（2009年）



全VPCが標準で備えているもの

- インスタンス等で使うプライベートIPアドレスの指定
- 既存のネットワークとの適合
- DHCPおよびDNS（Private DNS含む）
- Firewall
- 9001バイトのMTU
- APIを通じたプログラム制御、テンプレート、変更履歴、監査対応、フローログのサポート
- 実装は、パケットのカプセル化



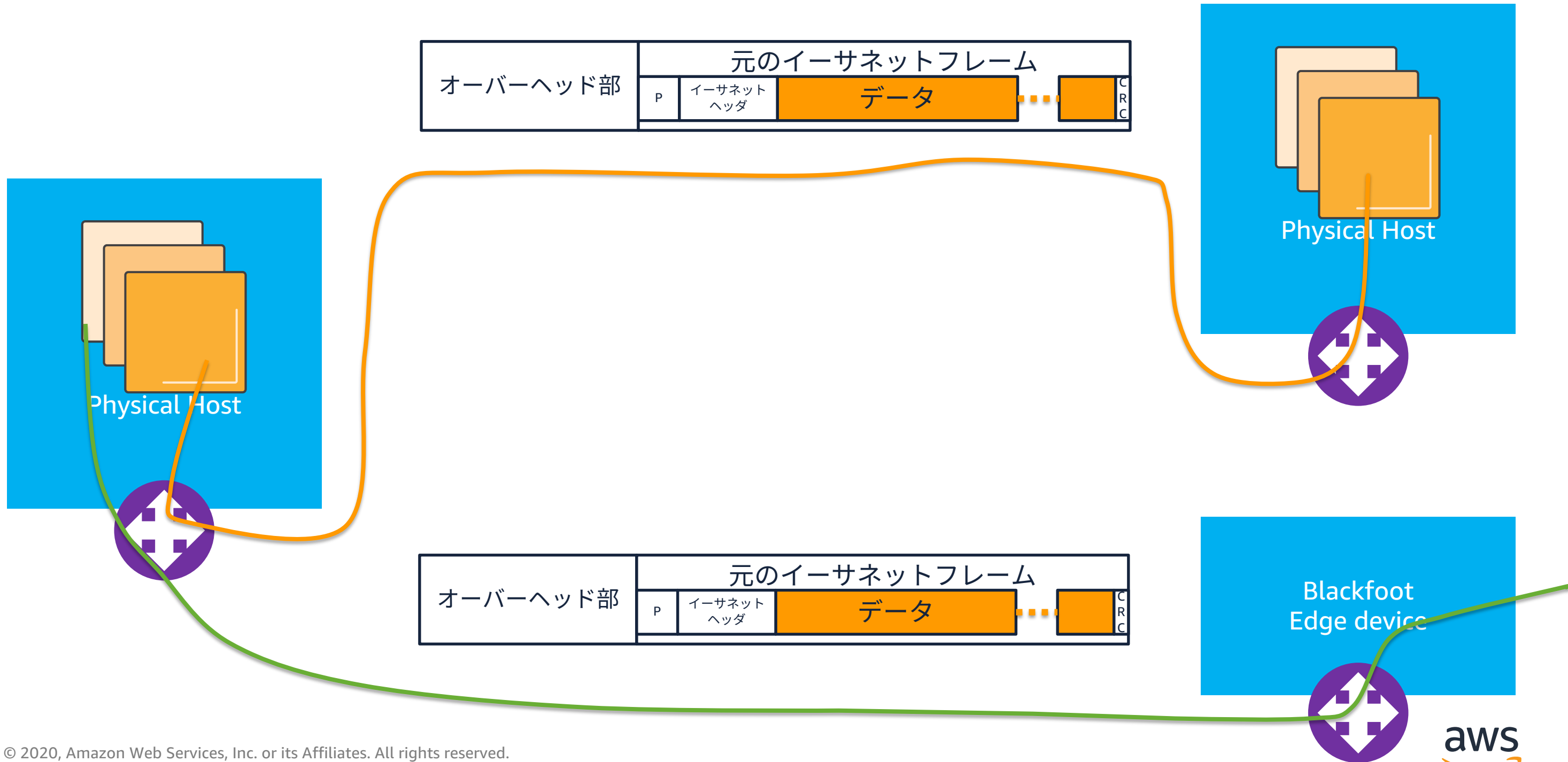
物理ホストのIP+VPCの各種機能（暗号化、ホスト情報などなど）に必要な情報を記述

4. インターネットにつながったクライアントからサーバへの旅

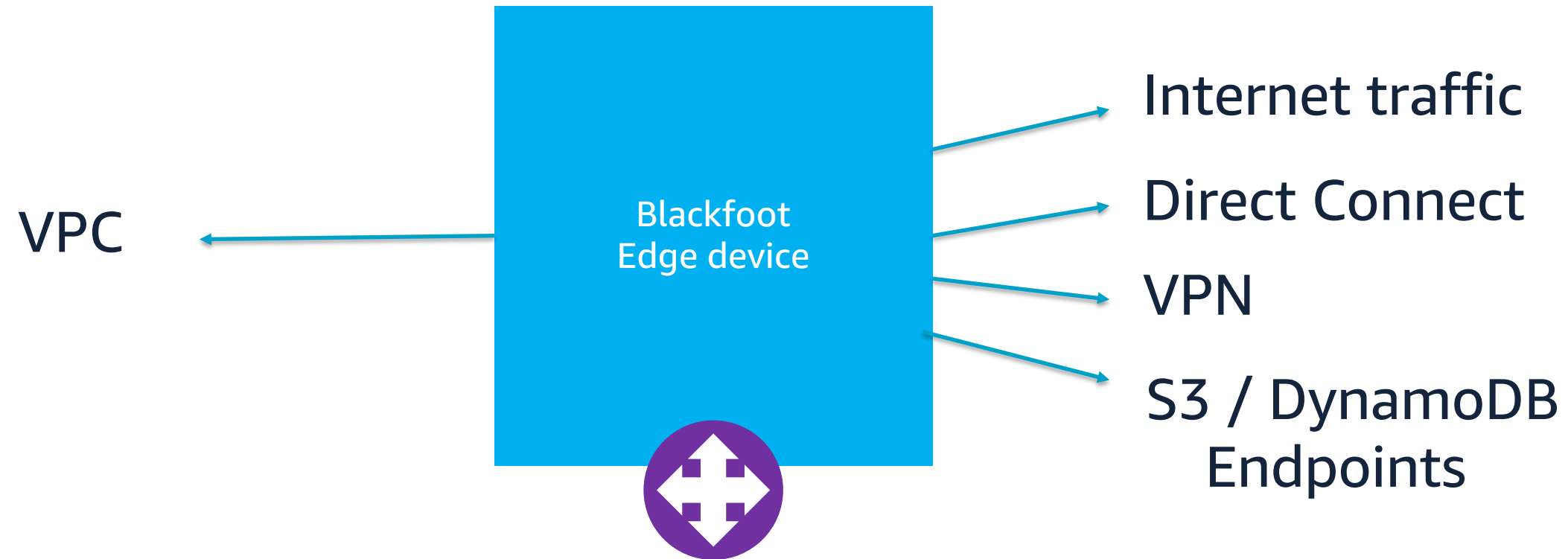
AWSのネットワークで一歩進んで知っておくべき10のこと

1. インスタンス起動からログインまで
2. インスタンスだけから見える専用ネットワークをつかって情報取得
3. Amazon Virtual Private Cloud (VPC)
4. インターネットにつながったクライアントからサーバへの旅
5. リージョンとインターネットのはざまで
6. AWSリージョンとグローバルバックボーン
7. VPC同士を接続する(VPC Peering, Transit Gateway, PrivateLink)
8. VPCとオンプレミスをつなぐ(VPNとDirect Connect)
9. インターネットからの攻撃とその対処
10. ハンズオン&ワークショップで復習

VPCと外の世界のゲートウェイ: Blackfoot



VPCと外の世界のゲートウェイ: Blackfoot

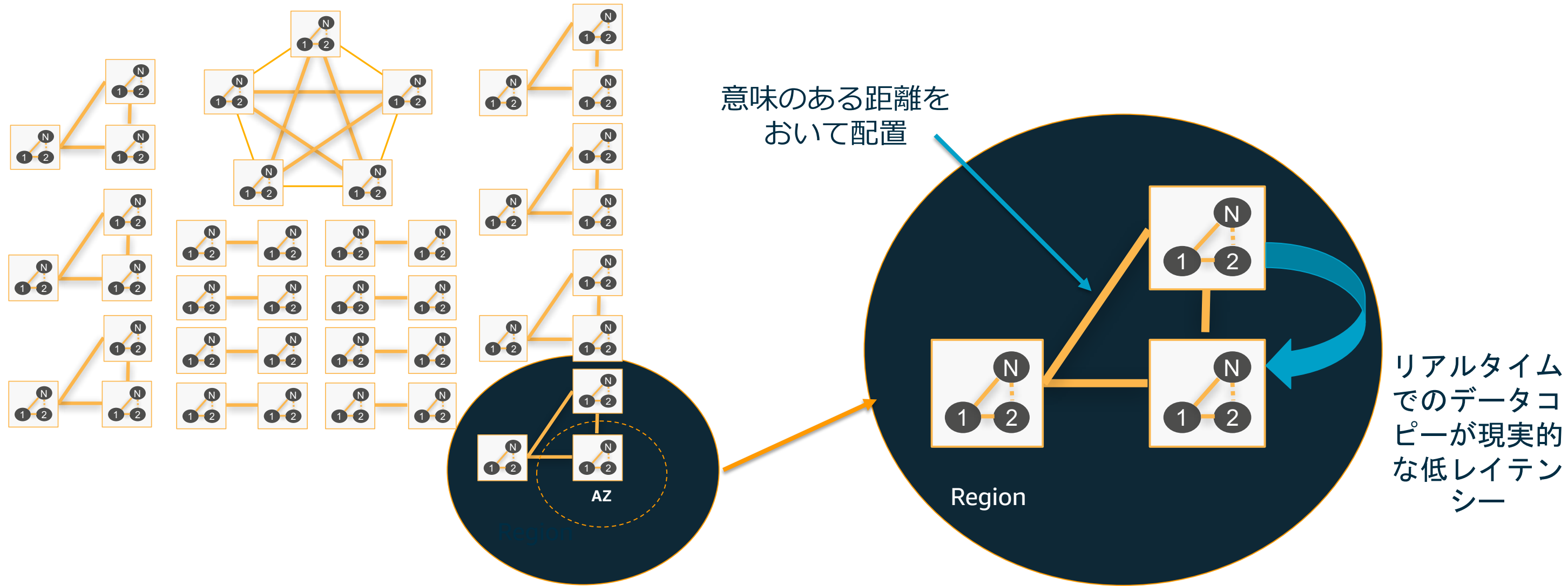


5. リージョンとインターネットのは ざまで

AWSのネットワークで一步進んで知っておくべき10のこと

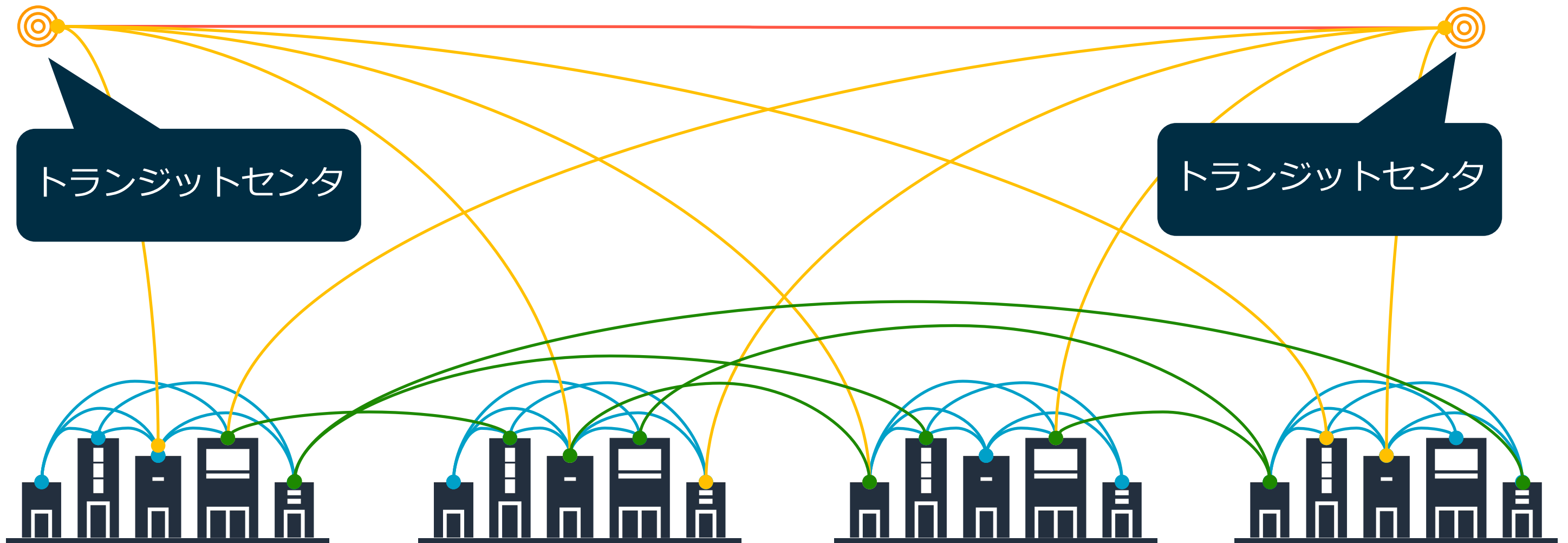
1. インスタンス起動からログインまで
2. インスタンスだけから見える専用ネットワークをつかって情報取得
3. Amazon Virtual Private Cloud (VPC)
4. インターネットにつながったクライアントからサーバへの旅
5. リージョンとインターネットのはざまで
6. AWSリージョンとグローバルバックボーン
7. VPC同士を接続する(VPC Peering, Transit Gateway, PrivateLink)
8. VPCとオンプレミスをつなぐ(VPNとDirect Connect)
9. インターネットからの攻撃とその対処
10. ハンズオン&ワークショップで復習

リージョンとアベイラビリティゾーン



AZは少なくとも2つのトランジットセンターで外部と接続

トランジットセンターは、インターネット、AWS Direct Connect、別リージョンとの結節点として機能



6.AWSリージョンとグローバル バックボーン

AWSのネットワークで一步進んで知っておくべき10のこと

1. インスタンス起動からログインまで
2. インスタンスだけから見える専用ネットワークをつかって情報取得
3. Amazon Virtual Private Cloud (VPC)
4. インターネットにつながったクライアントからサーバへの旅
5. リージョンとインターネットのはざまで
6. AWSリージョンとグローバルバックボーン
7. VPC同士を接続する(VPC Peering, Transit Gateway, PrivateLink)
8. VPCとオンプレミスをつなぐ(VPNとDirect Connect)
9. インターネットからの攻撃とその対処
10. ハンズオン&ワークショップで復習

いきなりですが Internetについて

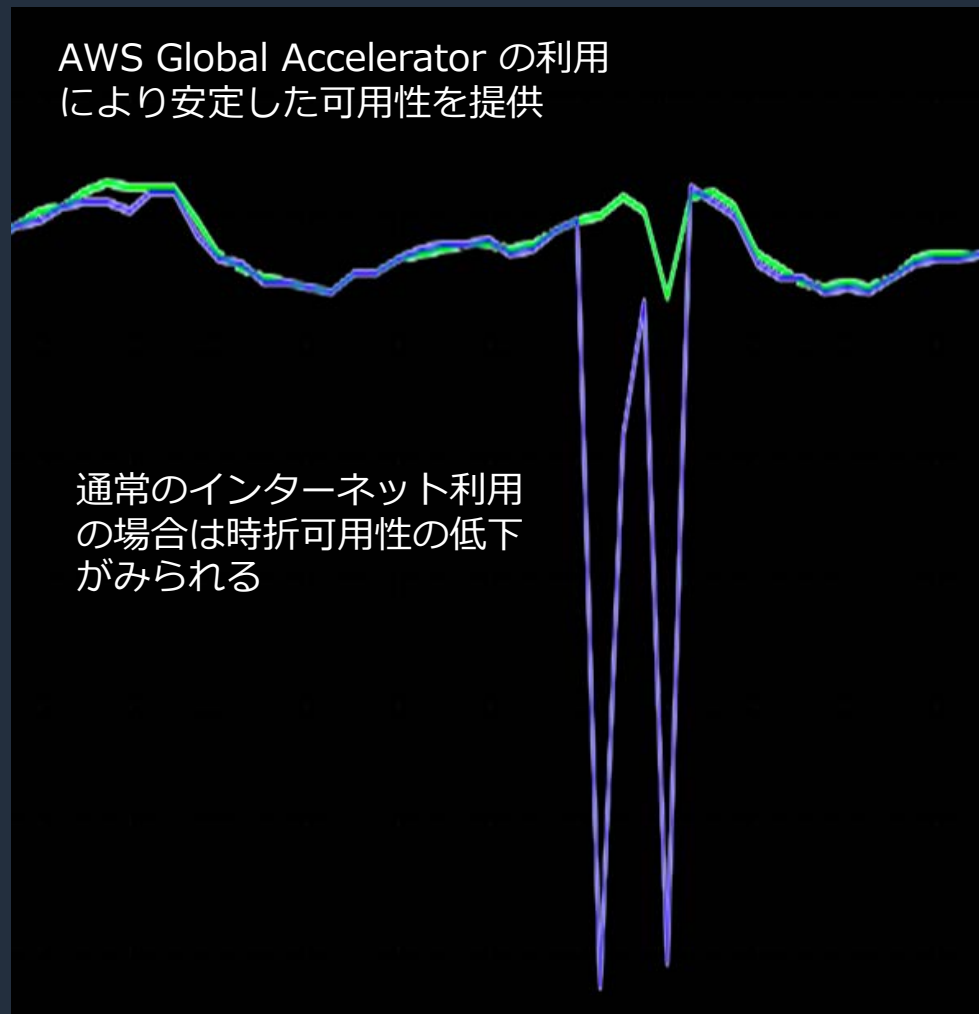


インターネットは複数のISPが集まった集合体 (network of networks) なので性能、可用性については全体では保証されていない

Internet の影響例と AWS Global Network の効果

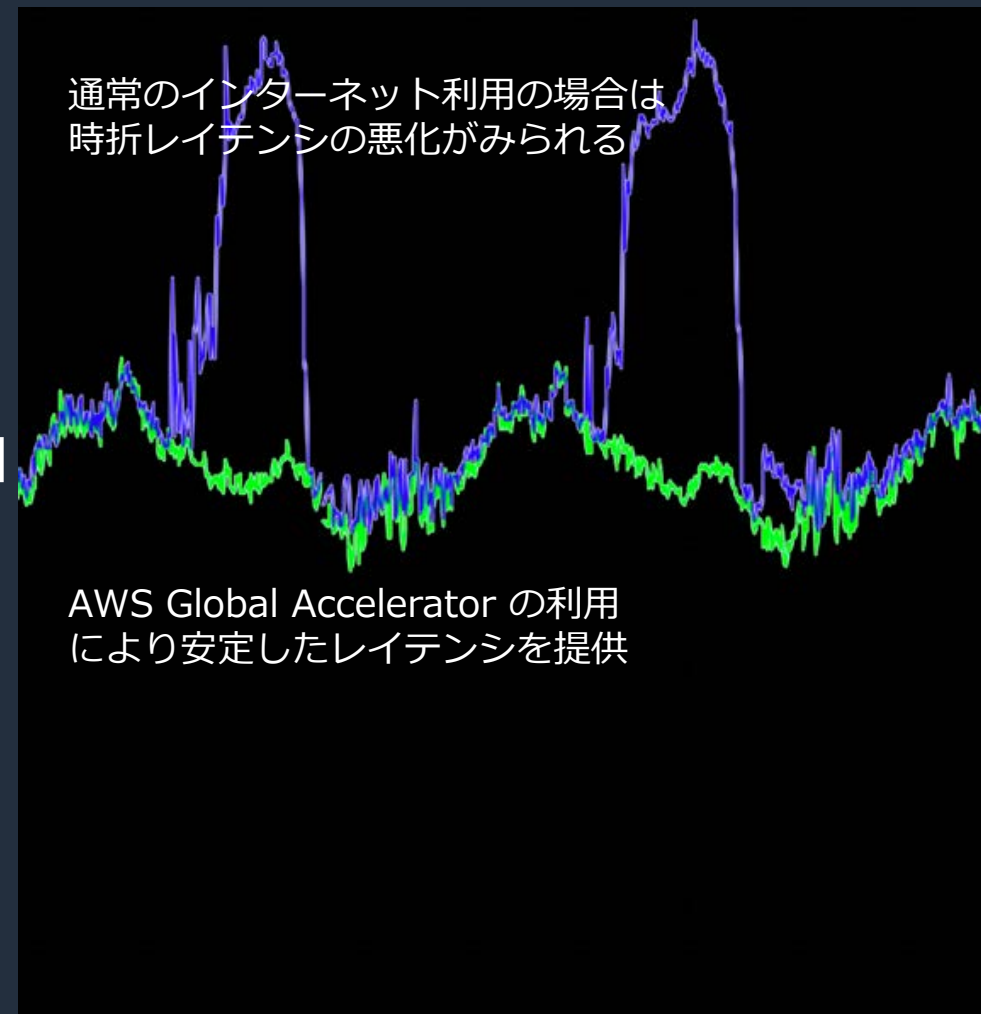
アメリカ国内での利用からスタート

Availability
(高いほどよい)



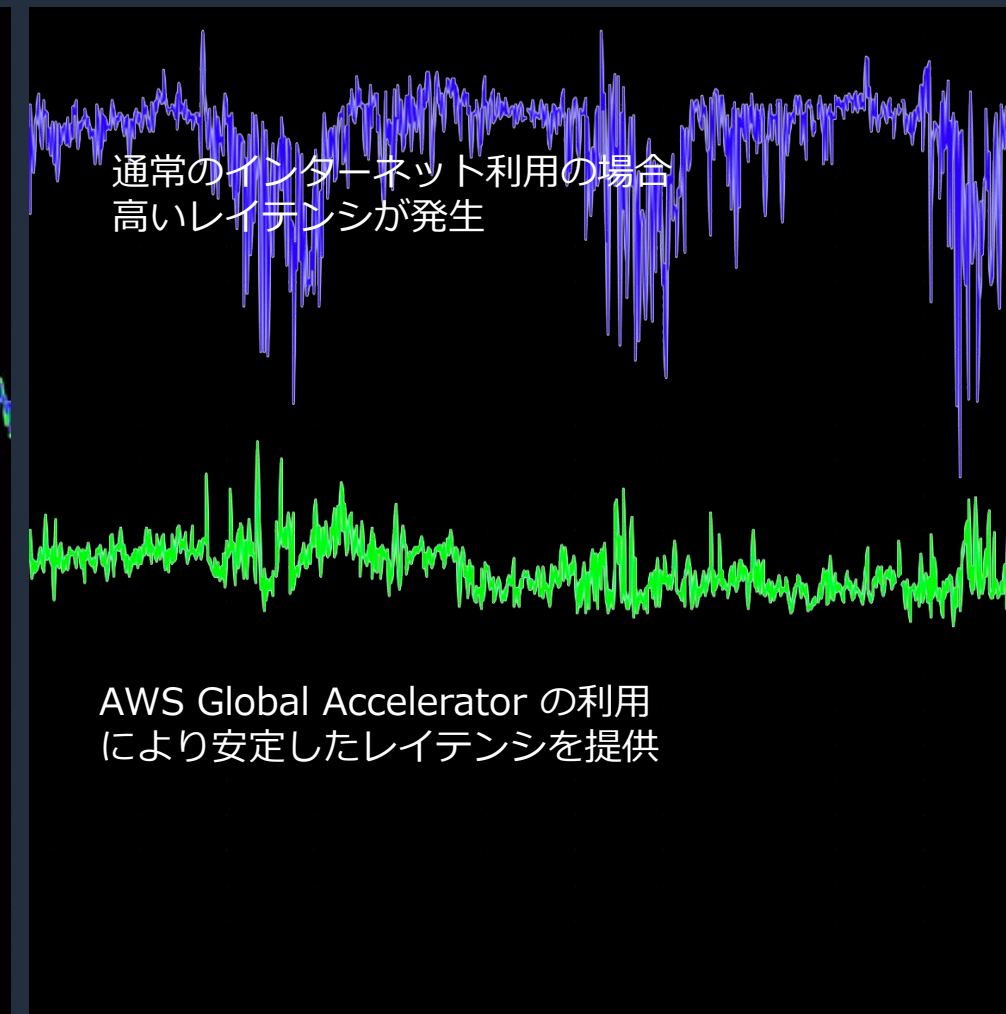
その後、ヨーロッパに展開

First byte latency
(低いほどよい)



さらに、アジアにも展開

First byte latency
(低いほどよい)



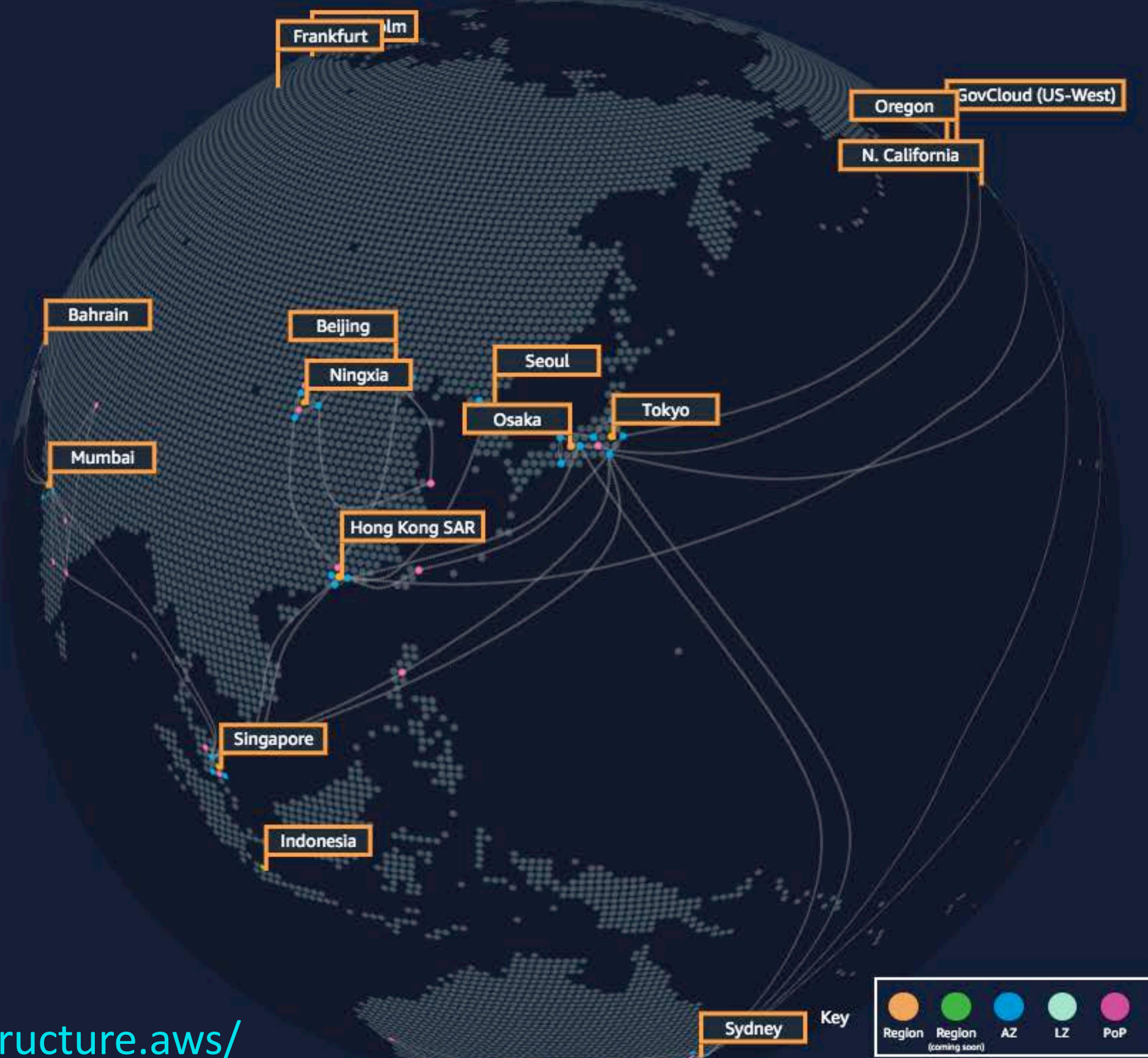


Projection Type



DISCOVER HOW WE DO IT

- Home >>
- Global Infrastructure >>>
- Regions >>>**
- Availability Zones >>>
- Local Zones >>>
- Points of Presence >>>
- Network >>
- Custom Hardware >>
- Benefits >>>

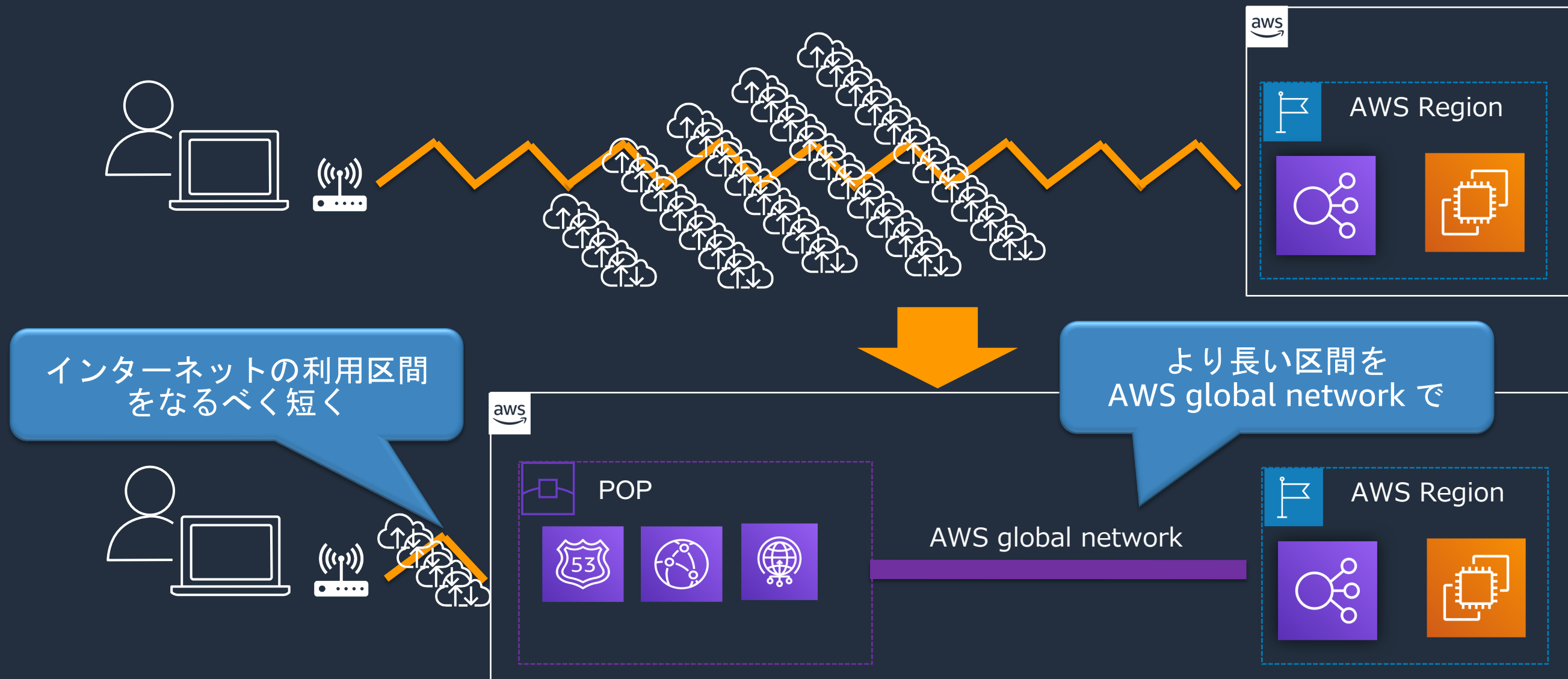


Key

- Region (orange circle)
- Region (coming soon) (green circle)
- AZ (blue circle)
- LZ (light blue circle)
- PoP (pink circle)
- Network (white circle)

<https://infrastructure.aws/>

AWS Global Network を利用するための AWS Edge Services



- エンドユーザにより近いところから配信(DNS,コンテンツ)
- AWS global network を利用することにより、より安定したユーザ体験を提供
- CloudFront のキャッシュも有効活用

Amazon Route 53

A reliable and cost-effective way to route end users to Internet applications

高い信頼性と拡張性を備えたマネージドクラウドドメインネームシステム (DNS)



高速

広域分散

100% SLA
(DNS Queries)

Zone Apex
サポート

ルーティング
ポリシー

ドメインレジスト
レーション

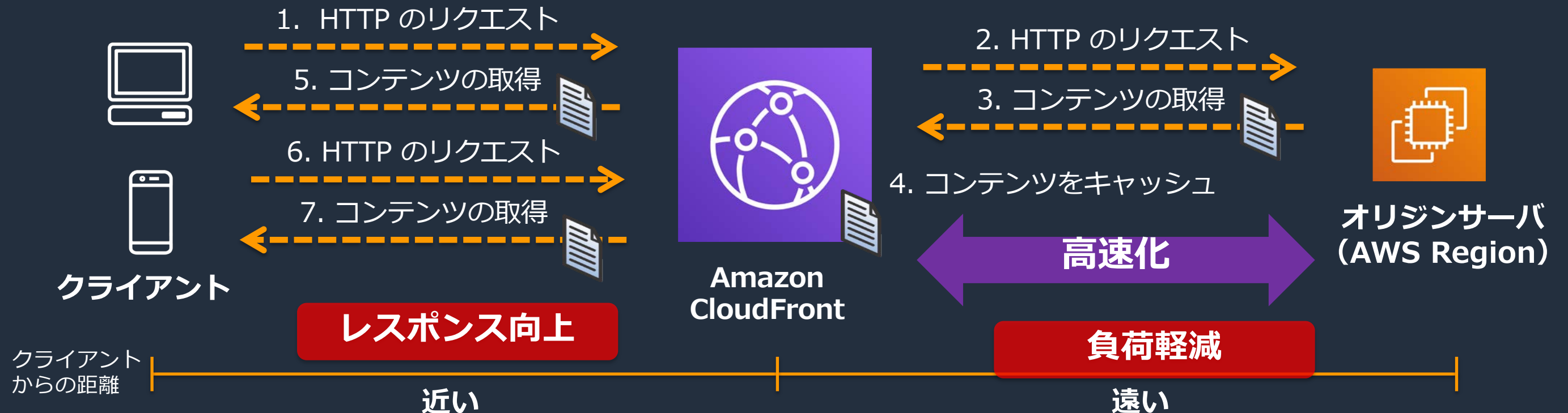
DNS はインターネットコミュニケーションにおける起点

Amazon CloudFront

Fast, highly secure and programmable content delivery network (CDN)

高い安全性と高性能な実現するプログラム可能なコンテンツデリバリーネットワーク

- ユーザーを一番近いエッジロケーションに誘導することで **配信を高速化**
- エッジサーバでコンテンツのキャッシングを行い **オリジンの負荷をオフロード**
- **AWS global network** を利用することによる非キャッシュコンテンツの高速化
- **Lambda@Edge** を利用することで柔軟な処理を実行可能



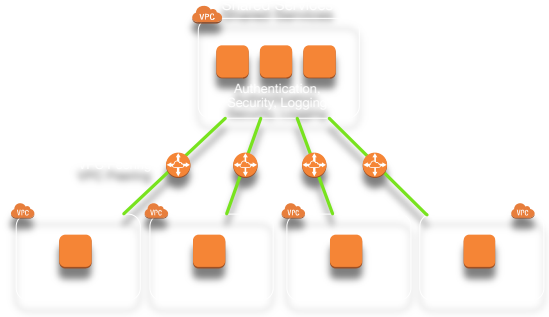
7.VPC同士を接続する(VPC Peering, Transit Gateway, PrivateLink)

AWSのネットワークで一歩進んで知っておくべき10のこと

1. インスタンス起動からログインまで
2. インスタンスだけから見える専用ネットワークをつかって情報取得
3. Amazon Virtual Private Cloud (VPC)
4. インターネットにつながったクライアントからサーバへの旅
5. リージョンとインターネットのはざまで
6. AWSリージョンとグローバルバックボーン
7. VPC同士を接続する(VPC Peering, Transit Gateway, PrivateLink)
8. VPCとオンプレミスをつなぐ(VPNとDirect Connect)
9. インターネットからの攻撃とその対処
10. ハンズオン&ワークショップで復習

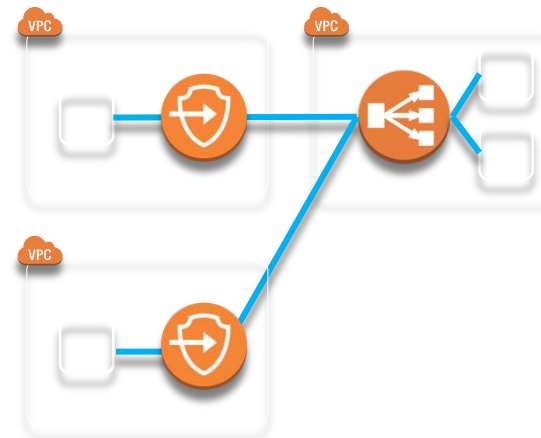
VPCの接続バリエーション

VPC peering



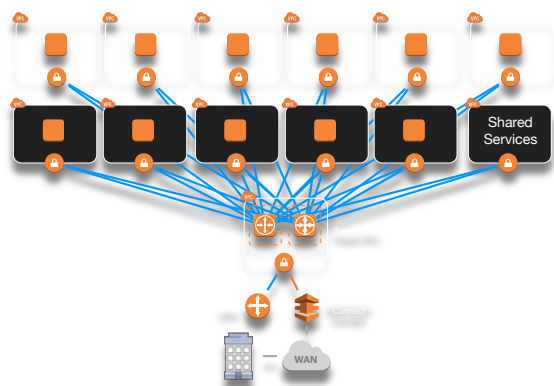
- 1 vs 1 の関係
- 100 VPCまで
- VPC間のSecurity groups
- Inter-region peering

AWS PrivateLink



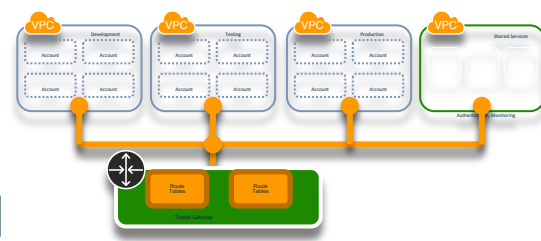
- 1 vs Nの関係
- スケーラブル
- IPアドレス重複でもOK
- NLBとエンドポイント費用

Transit VPC



- スポークの1つに配置
- 帯域の制限
- 制御が複雑
- インスタンスとライセンス費用

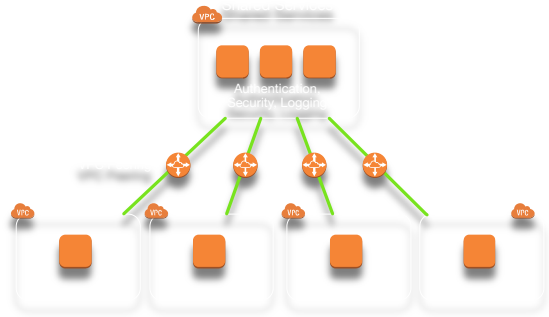
AWS Transit Gateway



- 1vs1でも1vsNでもroute table次第
- スケーラブル
- AZごとのエンドポイント費用

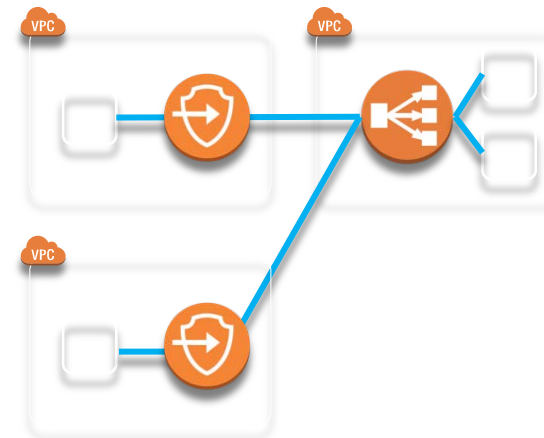
VPCのスケールする接続バリエーション

VPC peering



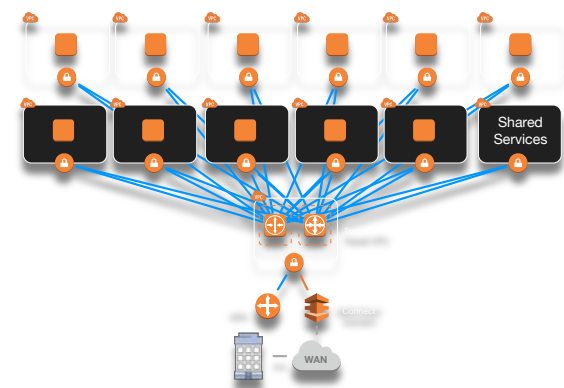
- 1 vs 1 の関係
- 100 VPCまで
- VPC間のSecurity groups
- Inter-region peering

✓ AWS PrivateLink



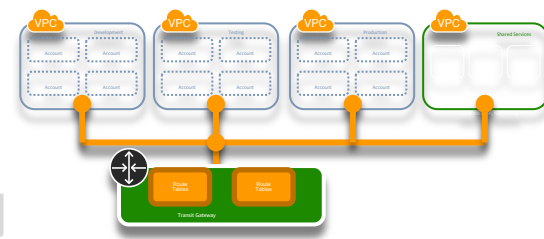
- スケーラブル

Transit VPC



- スポークの1つに配置
- 帯域の制限
- 制御が複雑
- インスタンスとライセンス費用

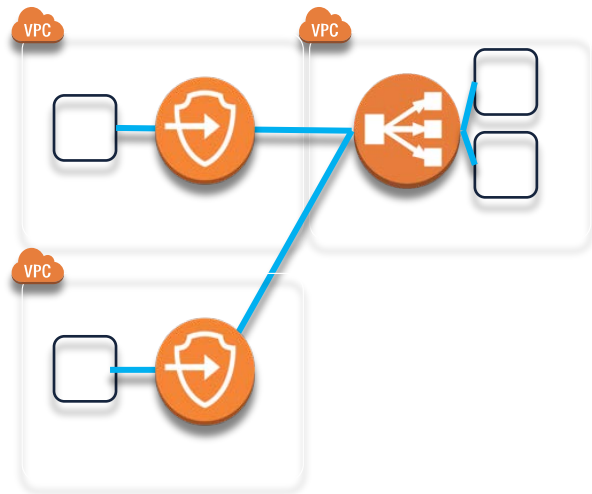
✓ AWS Transit Gateway



- スケーラブル

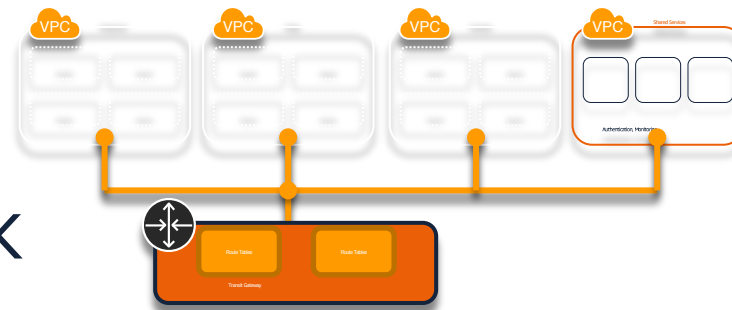
PrivateLinkとTransit Gateway

AWS PrivateLink



- 1 vs Nの関係
- スケーラブル
- IPアドレス重複でもOK
- NLBとエンドポイント費用

AWS Transit Gateway



- 1vs1でも1vsNでも route table次第
- スケーラブル
- AZごとのエンドポイント費用

Scope: アプリケーションの共用

Trust model: 相互信頼不要

Dependencies: NLB

Scale: 数千のVPCに対応

Scope: ネットワークの共用

Trust model: VPC間の信頼を集中管理

Dependencies: Transit Gateway

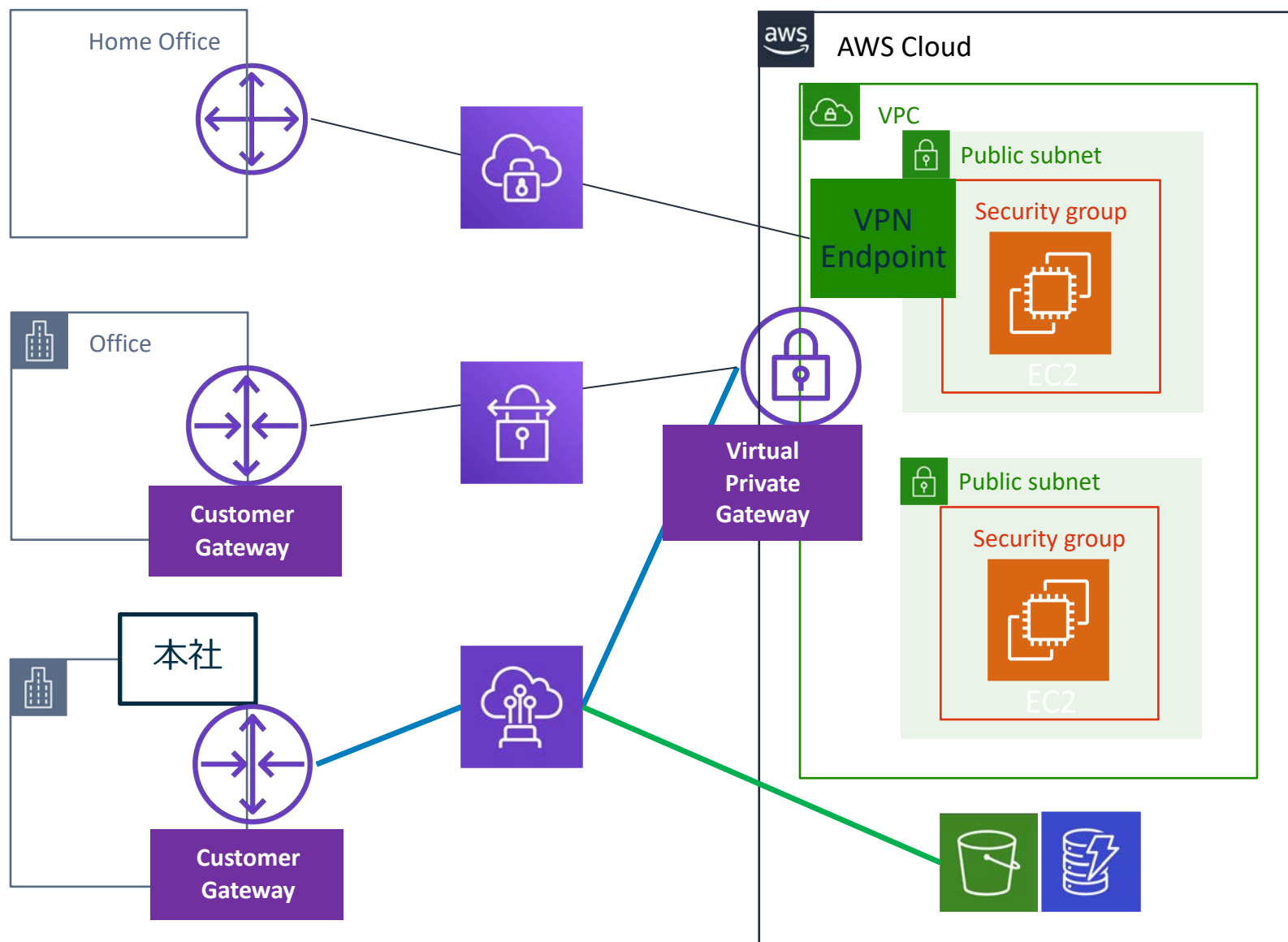
Scale: 数千のVPCに対応

8.VPCとオンプレミスをつなぐ (VPNとDirect Connect)

AWSのネットワークで一歩進んで知っておくべき10のこと

1. インスタンス起動からログインまで
2. インスタンスだけから見える専用ネットワークをつかって情報取得
3. Amazon Virtual Private Cloud (VPC)
4. インターネットにつながったクライアントからサーバへの旅
5. リージョンとインターネットのはざまで
6. AWSリージョンとグローバルバックボーン
7. VPC同士を接続する(VPC Peering, Transit Gateway, PrivateLink)
8. VPCとオンプレミスをつなぐ(VPNとDirect Connect)
9. インターネットからの攻撃とその対処
10. ハンズオン&ワークショップで復習

複数拠点からセキュアにVPCに接続



通信要件

- セキュアなサイト間接続
- 拠点間通信
- 回線の冗長化

サービス

- **Client VPN**
- **Site-to-Site VPN**
- **Direct Connect**

Client VPN

お客様のクライアントをOpenVPNベースのVPNを介してAWSへプライベートに接続するサービス

ユースケース

- 自宅や出張先からアクセスしたい

ポイント

- Active Directory を使用したクライアント認証と証明書ベースの認証をサポート
- VPCから他のVPC、AWSの各種サービス、オンプレミス、インターネットにシームレスにアクセス

Site-to-Site VPN

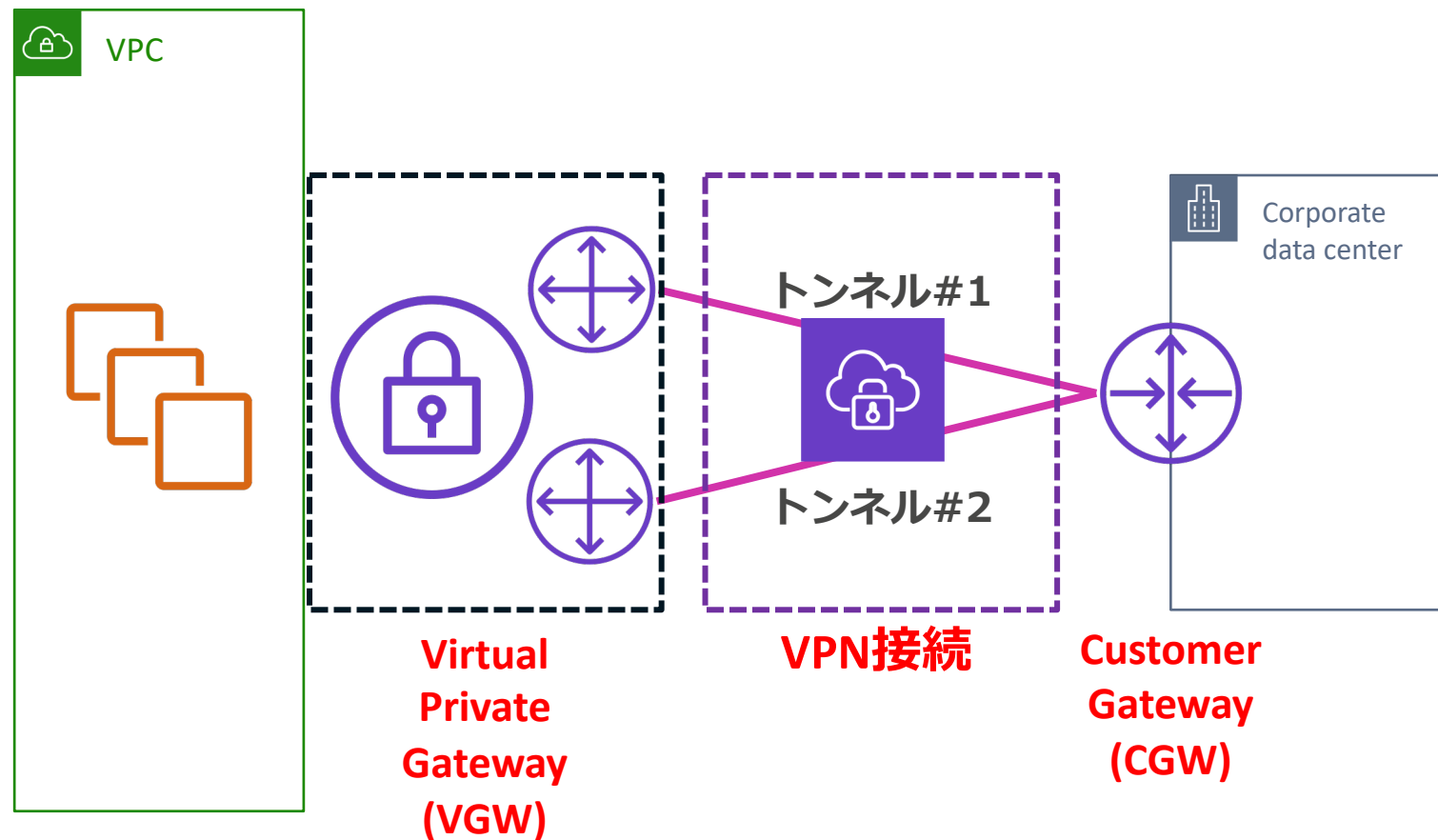
お客様のデータセンターやオフィスをIPsec VPNを介してAWSへプライベートに接続するサービス

Virtual Private GatewayもしくはTransit Gatewayと接続

ユースケース

- 拠点とAWSを簡単に早く接続したい
- 少量のトラフィック
- 価格重視/スモールスタート
- バックアップ回線

Site-to-Site VPNの接続構成



ポイント

- 1つのVPN接続は2つのIPsecトンネルで冗長化
- ルーティングは静的(スタティック)動的(ダイナミック:BGP)が選択可能
- VGWはDirect Connectのエンドポイントとしても利用
- IKEv2対応

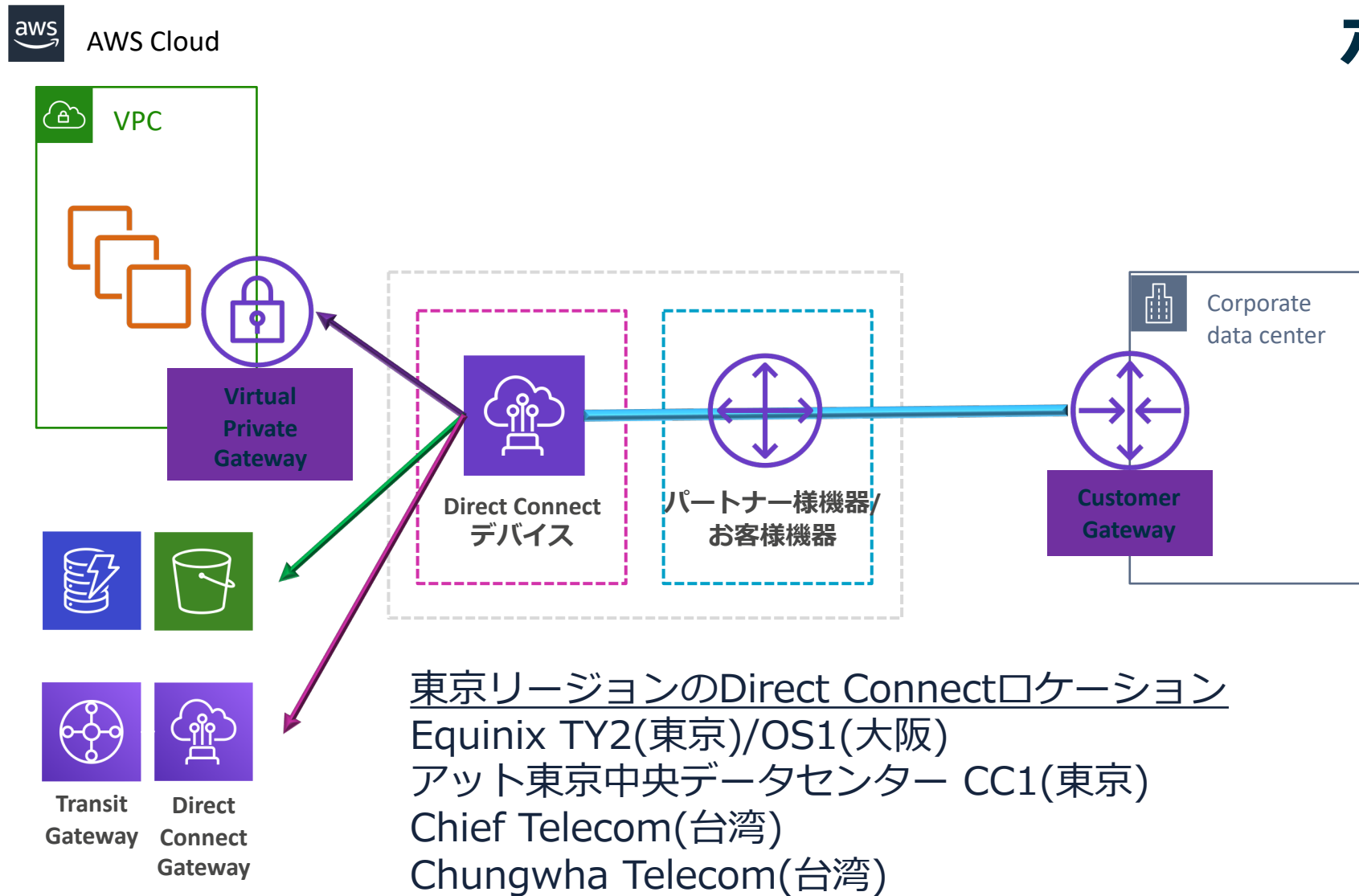
Direct Connect

お客様のデータセンターやオフィスを**専用線**を介してAWSへプライベートに接続するサービス

ユースケース

- 安定したパフォーマンスが必要
- 閉域網での接続が必要
- 大量のトラフィック
- 主回線
- 一貫性のある管理を実現したい

Direct Connectの接続構成



ポイント

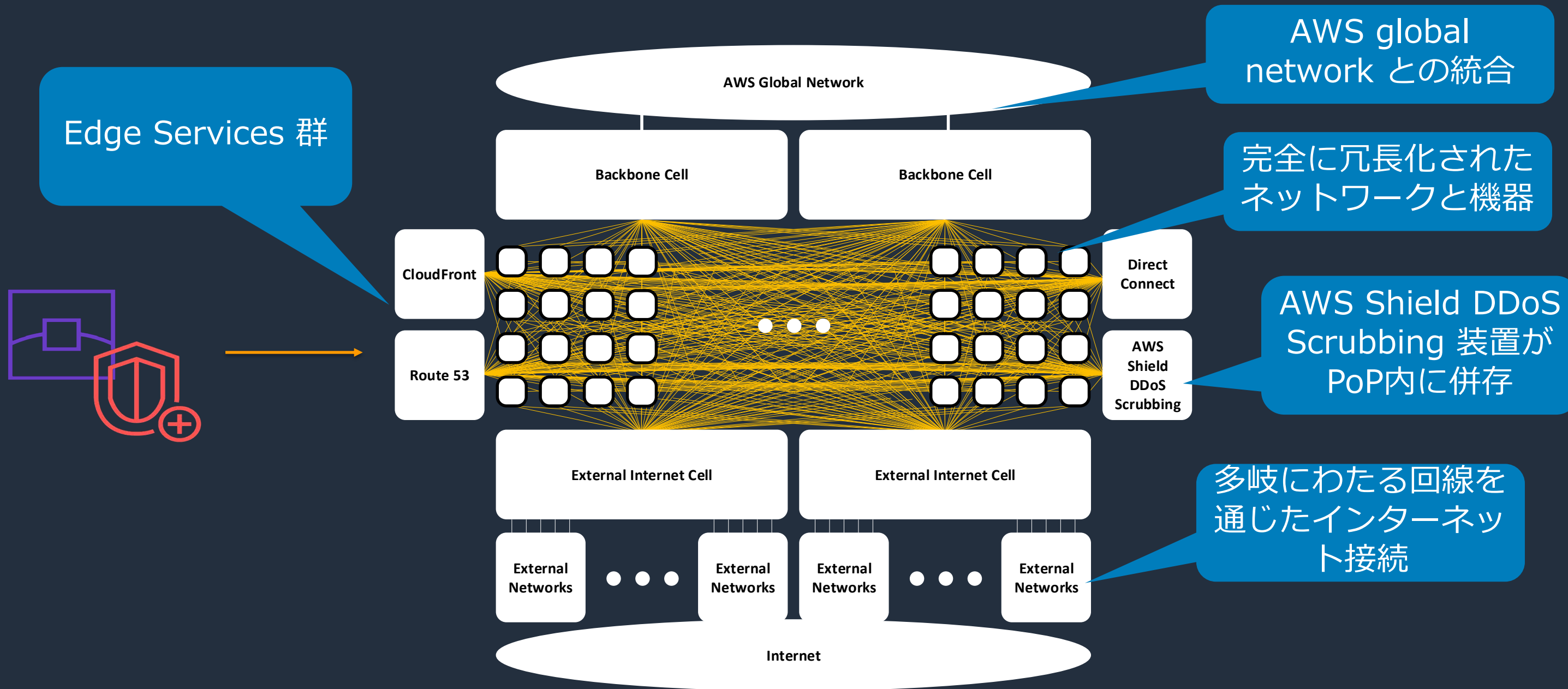
- オンプレミスから専用線を介してDirect Connect ロケーションに接続
- Direct Connect ロケーション = AWSクラウドへの物理的な接続を提供する拠点
- 物理接続を“Connections”、または“接続”と呼ぶ
- Connectionは1Gbpsまたは10Gbpsのポート速度をサポート
- ルーティングはBGPのみ
- 接続先は以下の3つ
 - VPC(プライベート接続)**
 - AWSクラウド(パブリック接続)**
 - TGW用のDXGW(トランジット接続)**

9. インターネットからの攻撃と その対処

AWSのネットワークで一歩進んで知っておくべき10のこと

1. インスタンス起動からログインまで
2. インスタンスだけから見える専用ネットワークをつかって情報取得
3. Amazon Virtual Private Cloud (VPC)
4. インターネットにつながったクライアントからサーバへの旅
5. リージョンとインターネットのはざまで
6. AWSリージョンとグローバルバックボーン
7. VPC同士を接続する(VPC Peering, Transit Gateway, PrivateLink)
8. VPCとオンプレミスをつなぐ(VPNとDirect Connect)
9. インターネットからの攻撃とその対処
10. ハンズオン&ワークショップで復習

In-line DDoS Mitigation Inside an Edge POP



AWS WAF

Protect your web applications from common web exploits

さまざまな攻撃から Web アプリケーションに対する防御を提供



マネージドルールと柔軟なカスタムルール



トラフィックフィルタリングとレートコントロール



モニタリング



廉価



迅速なデプロイ



フルAPIサポート

AWS Shield

Managed DDoS protection

高度な DDoS 攻撃からの保護を提供するマネージド DDoS 緩和サービス



大規模な DDoS 攻撃
からの保護



検出とモニタリング項目の追加



攻撃の検知と緩和状況を可視化



コスト保護 (DDoSによる
コストの吸収)



24x7
Security Response Team
(SRT)



AWS WAF と FW
Manager のバンドル

AWS Firewall Manager

Centrally configure and manage firewall rules across accounts and applications

AWS Organizations のアカウント/アプリケーションで一元的にファイアウォールのルールを設定/管理



AWS Organizations
全体での対応



セキュリティ管理者に対する
単一アクセスポイントの提供



必須ルールの適用などポリ
シーの集中管理/設定



AWS Security Hubとの連
携などAWSのセキュリテイ
サービスとの連携



ポリシーの適用状況の管理



ダッシュボードによる
可視化

10. ハンズオン&ワークショップで 復習

AWSのネットワークで一步進んで知っておくべき10のこと

1. インスタンス起動からログインまで
2. インスタンスだけから見える専用ネットワークをつかって情報取得
3. Amazon Virtual Private Cloud (VPC)
4. インターネットにつながったクライアントからサーバへの旅
5. リージョンとインターネットのはざまで
6. AWSリージョンとグローバルバックボーン
7. VPC同士を接続する(VPC Peering, Transit Gateway, PrivateLink)
8. VPCとオンプレミスをつなぐ(VPNとDirect Connect)
9. インターネットからの攻撃とその対処
10. ハンズオン&ワークショップで復習

AWSデータセンターバーチャルツアー

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

AWS のデータセンター

AWS は2006年からクラウドコンピューティングの先駆者として、セキュアにシステムを構築し、素早くイノベーションを起こすことが可能なクラウドのインフラストラクチャーを創造してきました。AWS はデザイン上、あるいは自然災害や人為的なリスクから AWS のインフラストラクチャーを保護するための AWS のデータセンターシステムについて、継続したイノベーションに取り組んでいます。また、AWS ではセキュリティやコンプライアンス上の統制を実装し、オートメーション・システムを構築し、第三者監査によるセキュリティやコンプライアンスについての検証を実施しています。その結果、世界で最も厳しく規制されている組織からも信頼をいただいています。膨大な数の実際にご利用いただいているお客様を保護するためのセキュリティ上の取り組みについて知っていただくために、AWS のデータセンターの一部をご紹介しますバーチャルなツアーにご参加ください。



境界防御レイヤー

AWS のデータセンターの物理的なセキュリティは、境界防御線から開始されます。このレイヤーはいくつもの特徴的なセキュリティ要素を含んでおり、物理的な位置によって、保安要員、防御壁、侵入検知テクノロジー、監視カメラ、その他セキュリティ上の装置等が存在します。

[詳しく見る >](#)



インフラストラクチャー・レイヤー

インフラストラクチャー・レイヤーにはデータセンターの建屋、各種機械、およびそれらの運用に係るシステムが存在します。電力ジェネレーターや冷暖房換気空調設備、消化設備等といった機械や設備は、すべてインフラストラクチャー・レイヤーに含まれます。

[詳しく見る >](#)



AWS データセンターのセキュアな設計について (日本語)

https://youtu.be/1-Bbe9_7J4o



データレイヤー

データレイヤーは、カスタマーデータを保持する唯一のエリアとなるため、防御の観



環境レイヤー

環境レイヤーは、立地の選択、建設、運

<https://infrastructure.aws/>

The screenshot displays the AWS Infrastructure website interface. On the left, a navigation menu lists various options: Home, Global Infrastructure, Regions (highlighted in orange), Availability Zones, Local Zones, Points of Presence, Network, Custom Hardware, and Benefits. The main content area features a world map with colored dots representing different regions, with 'Osaka' and 'Tokyo' highlighted. In the top right corner, there is a 'Projection Type' section with globe and map icons. A text box in the upper right contains the Japanese text: 'ブラウザでインタラクティブにAWSのインフラ情報を記述'. A popup window titled 'Tokyo' with a close button (X) is open, showing '4 Availability Zones' and a photograph of the Tokyo skyline at dusk.

ブラウザでインタラクティブにAWSのインフラ情報を記述

Tokyo X
4 Availability Zones

A photograph of the Tokyo skyline at dusk, featuring the Tokyo Skytree and various city buildings illuminated against a twilight sky.

AWS Global Accelerator Speed Comparison

<https://speedtest.globalaccelerator.aws/>

AWS Global Accelerator Speed Comparison

About this tool

[AWS Global Accelerator](#) is a service that improves the availability and performance of your applications. This tool compares Global Accelerator to the public internet. Choose a file size to see the time to download a file from application endpoints in different AWS Regions to your browser.

Files are downloaded over HTTPS/TCP from Application Load Balancers (ALBs) in different AWS Regions to your browser. [Learn more](#)

Choose a file size and click "Start" to start the tests:

We welcome suggestions for how to improve this tool. [Provide feedback](#)

i Results may differ when you run the test multiple times. Download times can vary based on factors that are external to Global Accelerator, such as the quality, capacity, and distance of the connection in the last-mile network that you're using.

N. Virginia (us-east-1)

Direct over internet



AWS Global Accelerator



Oregon (us-west-2)

Direct over internet



Total time
2834ms

AWS Global Accelerator



1989ms

30% faster with AWS Global Accelerator

Ireland (eu-west-1)

Direct over internet



AWS Global Accelerator



Amazon S3 Transfer Acceleration Speed Comparison

<https://s3-accelerate-speedtest.s3-accelerate.amazonaws.com/en/accelerate-speed-comparision.html>



Amazon S3 Transfer Acceleration Speed Comparison

Upload speed comparison in the selected region

Virginia

(US-EAST-1)

72% faster

S3 Direct Upload Speed



Upload complete

S3 Accelerated Transfer Upload Speed



Upload complete

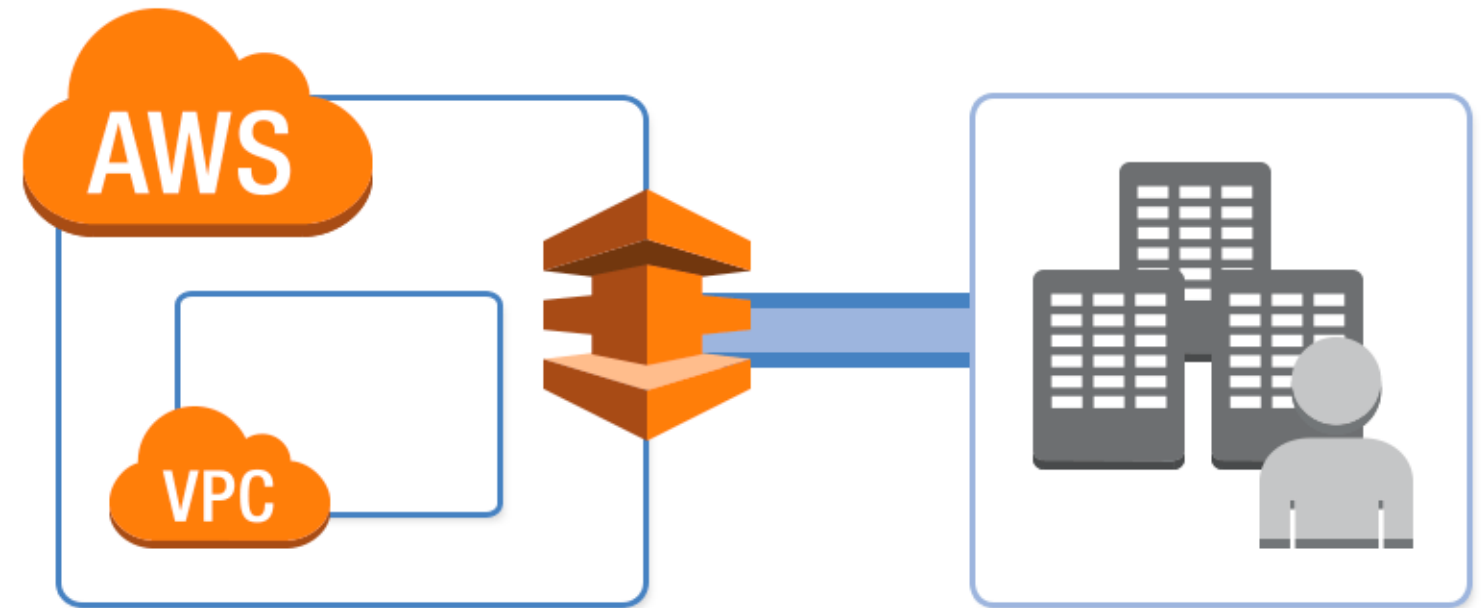
This speed checker uses multipart uploads to transfer a file from your browser to various Amazon S3 regions with and without Amazon S3 Transfer Acceleration. It compares the speed results and shows the percentage difference for every region.

Note: In general, the farther away you are from an Amazon S3 region, the higher the speed improvement you can expect from using Amazon S3 Transfer Acceleration. If you see similar speed results with and without the acceleration, your upload bandwidth or a system constraint might be limiting your speed.

AWS 専用線アクセス体験ラボトレーニング

https://aws.amazon.com/jp/dx_lab/

AWS 専用線アクセス体験ラボ

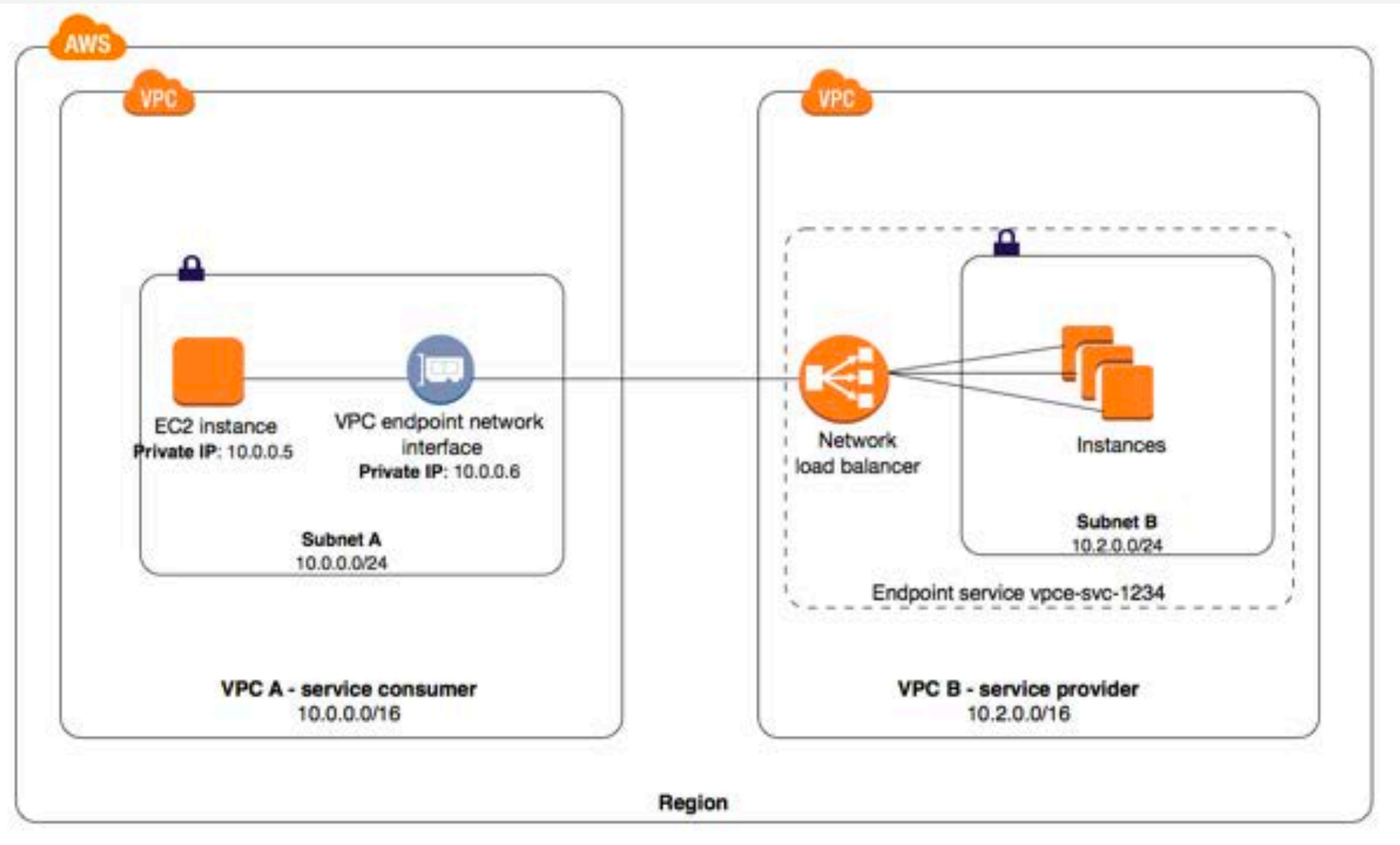


Direct Connect Gatewayを用いて複数リージョンとオンプレミスを接続する過程を体験いただきます。

AWS主催のハンズオンセミナーにて環境利用時に必要なトークンコードを配布。セミナー実施時以外には、自身でDirect Connectを利用できる環境が必要。

SaaSを自分のVPC内で使う方法(PrivateLink)

<https://aws-saas-privatelink.workshop.aws/>

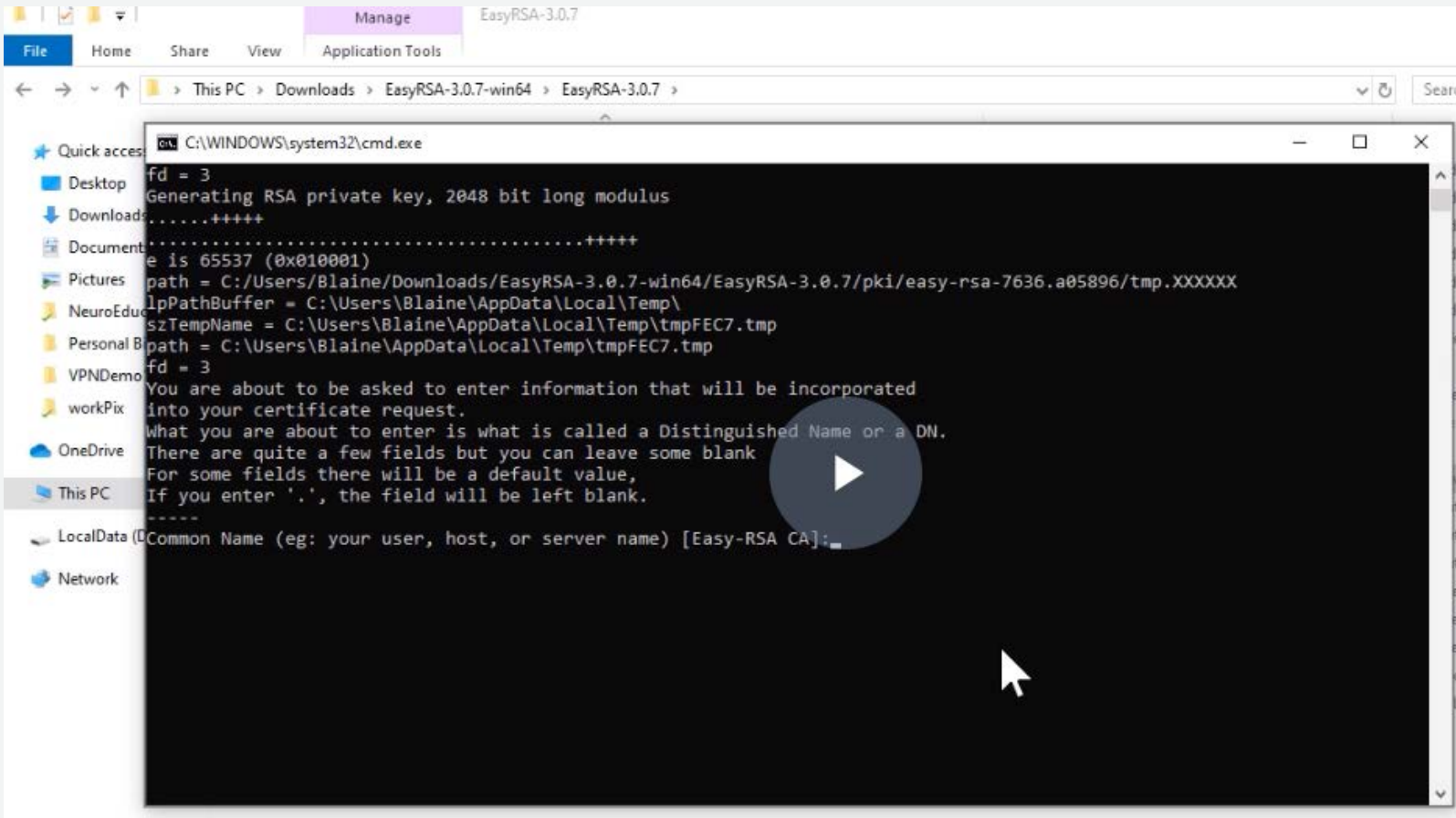


AWS PrivateLinkは、他のAWS VPCに対して安全にサービスを提供する手法です。このハンズオンでは、2つのVPCをSaaSのサービス提供者、受給者に分け、それぞれが必要な手順を体験いただきます。

1. CloudFormationで2つのVPCを作成。プロバイダVPC内にNLB配下のnginxを設置。
2. PrivateLinkでVPCエンドポイントサービスを作成
3. クライアントVPCではエンドポイントを作成
4. プロバイダVPCではエンドポイント接続リクエストを承諾
5. クライアントVPCから動作確認

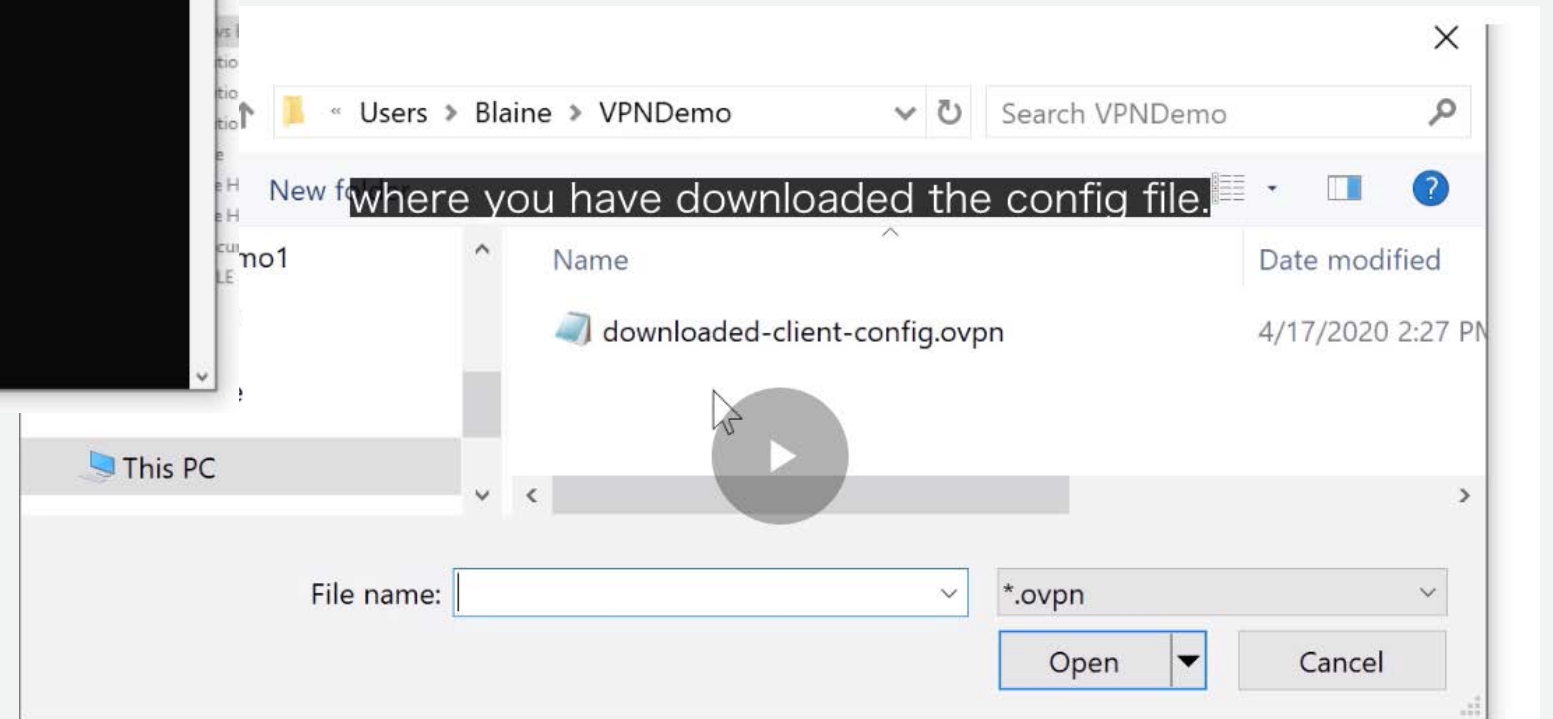
Configure and Deploy AWS Client VPN

<https://go.aws/2Z1R4QM> での動画解説



クライアント側

1. aws.amazon.com/vpn/client-vpn-downloadからインストール
2. .ovpnファイルを読み込んで接続



サーバ側

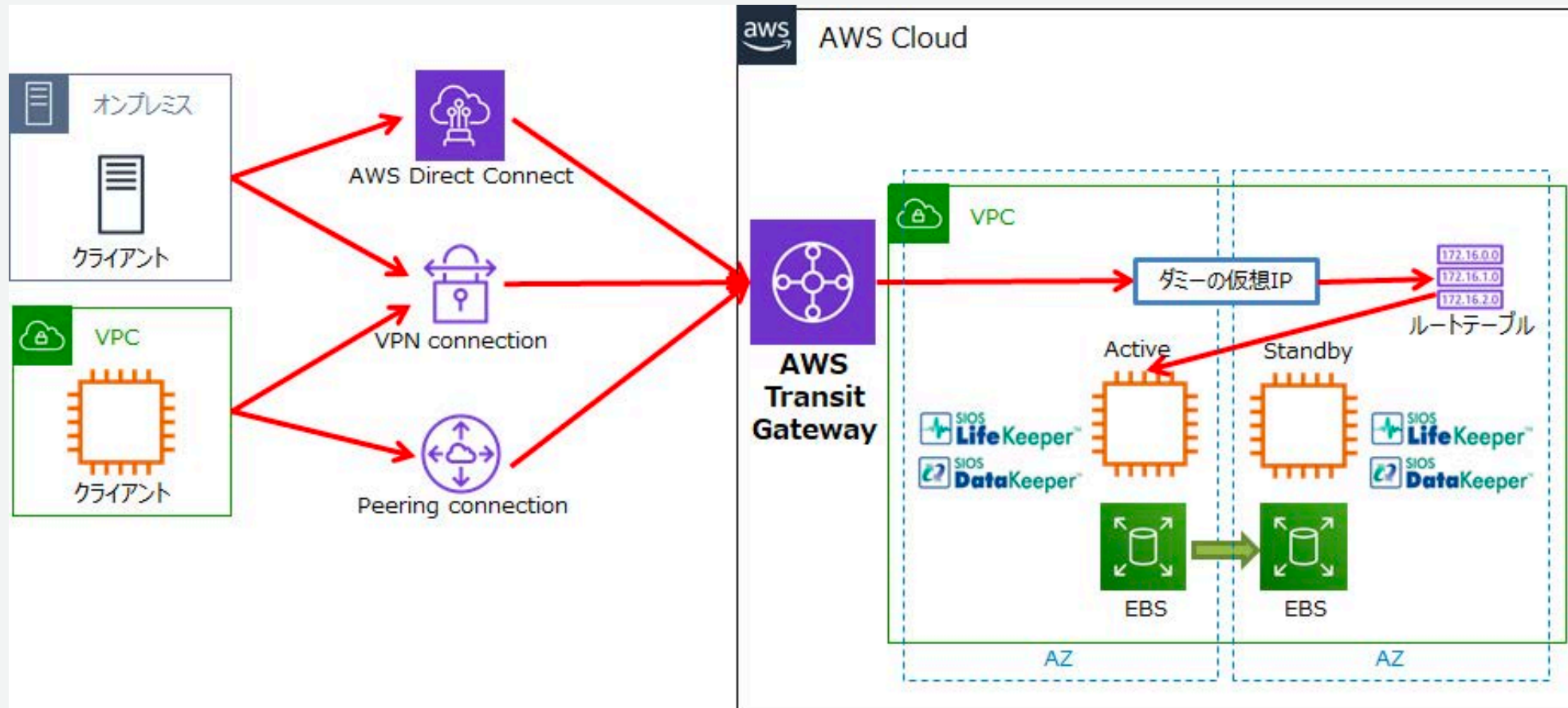
1. GithubにあるEasyRSA-Start.batをつかってサーバとクライアント証明書を作成
2. Client VPNエンドポイントの作成
3. OpenVPNの設定ファイル(.ovpnファイル)作成



AWS Transit Gatewayを使用したHAクラスター構成

<https://bcblog.sios.jp/aws-transit-gateway-ha/> での動画解説

<https://youtu.be/3lExuneoQ84>



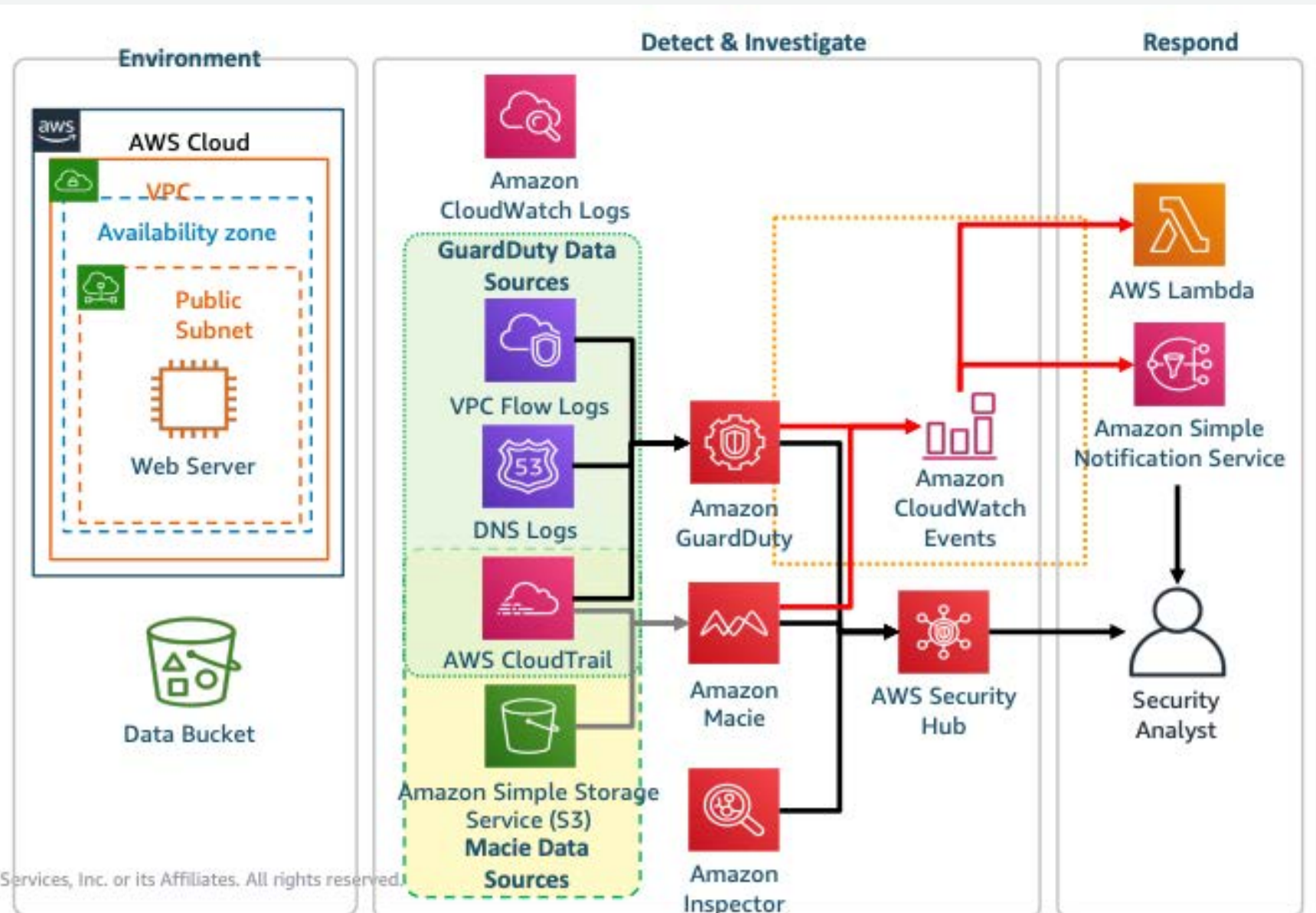
接続方式の違いをTransit Gatewayが吸収

ビデオの内容

1. AWS TransitGatewayについて
2. TransitGatewayを使わないHAクラスター構成
3. TransitGatewayを使ったHAクラスター構成

AWS 環境における脅威検知と対応

<https://scaling-threat-detection.awssecworkshops.jp/>



1. CloudFormationで環境構築
2. 攻撃シミュレーション
3. 検知と対応
4. レビュー&ディスカッション

サービス環境は単一インスタンスの単純なインターネット公開サーバ

サービス環境

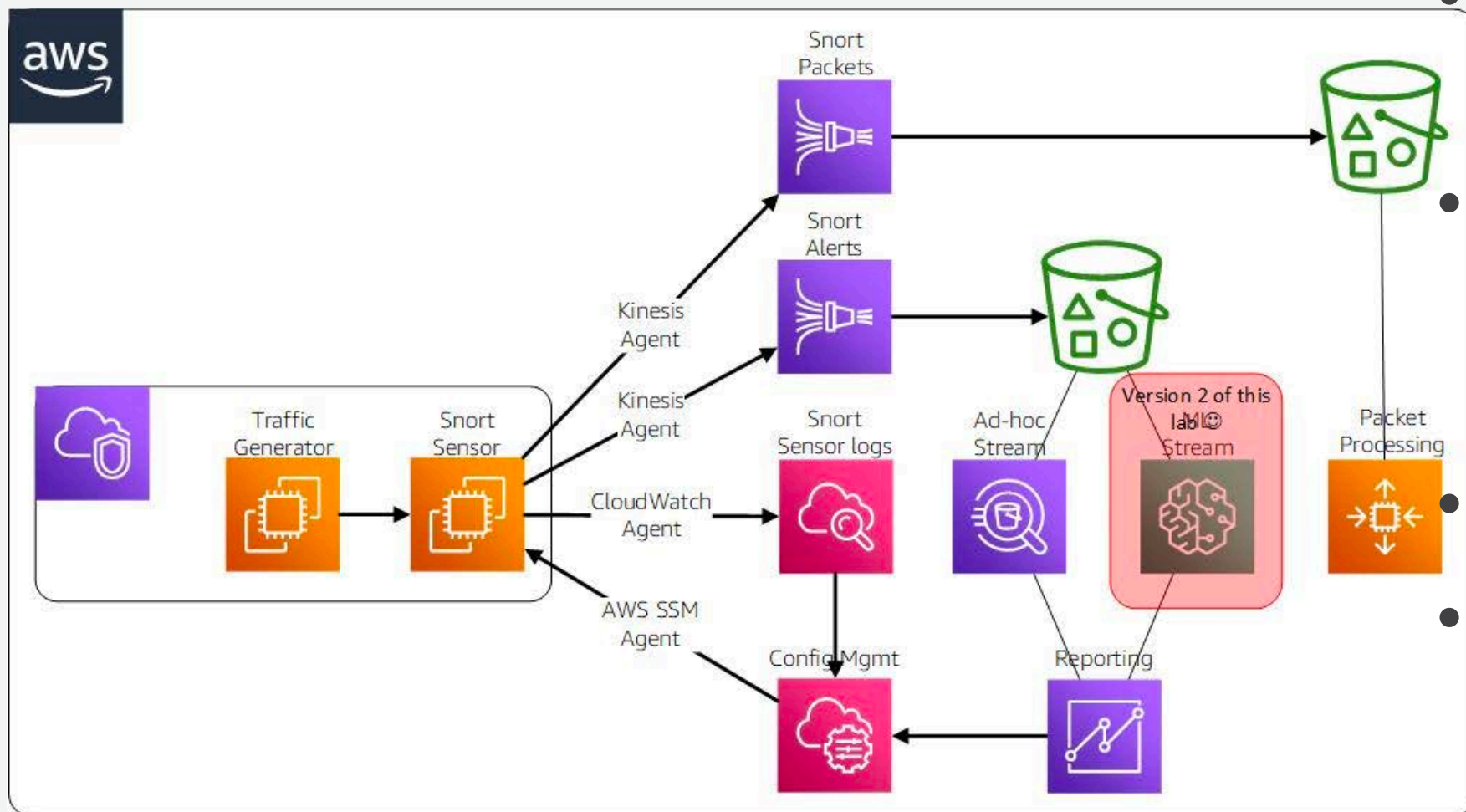
脅威検知環境

脅威対応環境



Intelligent Automation with AWS and Snort IDS

<https://github.com/aws-samples/aws-reinvent-2019-builders-session-opn215>



- 多数のSnortセンサーをSSM Agentで制御
- Kinesis Data Firehoseを使ってSnortのアラートとパケットを収集
- S3にデータ蓄積
- AthenaとQuickSightで分析



おわりに

まとめ：

AWSのネットワークで一歩進んで知っておくべき10のこと

1. インスタンス起動からログインまで
2. インスタンスだけから見える専用ネットワークをつかって情報取得
3. Amazon Virtual Private Cloud (VPC)
4. インターネットにつながったクライアントからサーバへの旅
5. リージョンとインターネットのはざままで
6. AWSリージョンとグローバルバックボーン
7. VPC同士を接続する(VPC Peering, Transit Gateway, PrivateLink)
8. VPCとオンプレミスをつなぐ(VPNとDirect Connect)
9. インターネットからの攻撃とその対処
10. ハンズオン&ワークショップで復習



Thank You !

AWSのネットワークで一步進んで知っておくべき10のこと

1. インスタンス起動からログインまで
2. インスタンスだけから見える専用ネットワークをつかって情報取得
3. Amazon Virtual Private Cloud (VPC)
4. インターネットにつながったクライアントからサーバへの旅
5. リージョンとインターネットのはざまで
6. AWSリージョンとグローバルバックボーン
7. VPC同士を接続する(VPC Peering, Transit Gateway, PrivateLink)
8. VPCとオンプレミスをつなぐ(VPNとDirect Connect)
9. インターネットからの攻撃とその対処
10. ハンズオン&ワークショップで復習

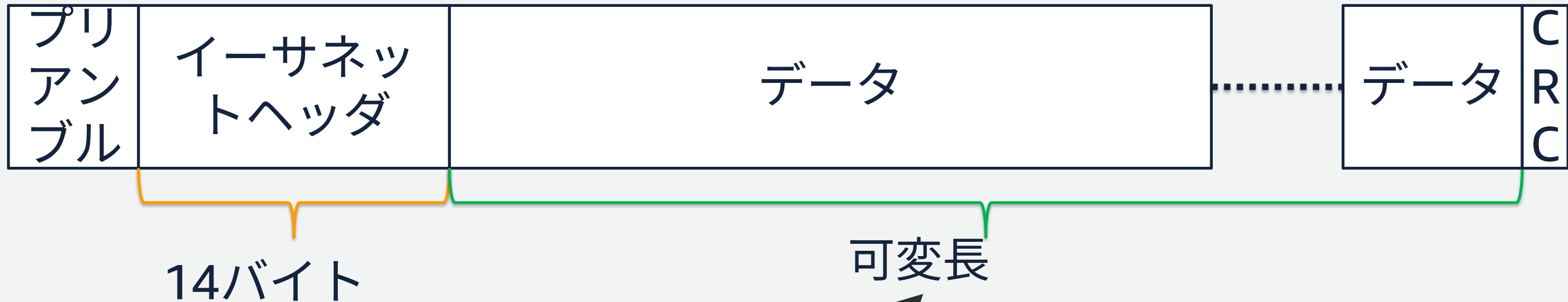
VPCがどのように動作しているのか

Virtual Networkingのシンプルな実現法

Subnet \approx VLAN

VPCと外をつなぐ \approx VRF (virtual routing and forwarding)

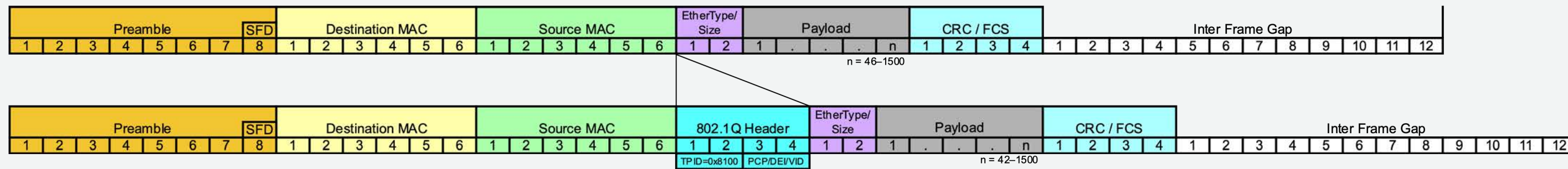
イーサネットの基本フレーム



実際にはイーサネット標準の
1500までとなることが多い

IEEE 802.1Q VLAN

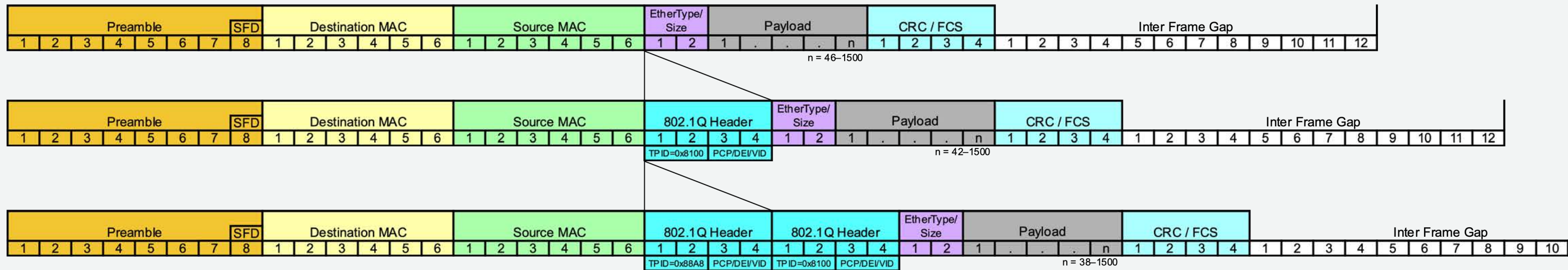
元のフレームをカプセル化せずに4バイトのヘッダを追加



+4094までのテナント対応
-4バイトのオーバーヘッド

IEEE 802.1ad

元のフレームをカプセル化せずに4バイトのヘッダを追加後、さらに4バイトずつタギングする



+4094x4094までのテナント対応

-8バイトのオーバーヘッド

問題とAWS VPCでのアプローチ

Subnet ~= VLAN

- VLAN IDスペースが小さすぎる (12ビット=4096)

VPCと外をつなぐ ~= VRF

- 大きなルータでも数千のオーダー



加えて、、ベンダのバグ修正には数ヶ月かかることに悩んでいたAmazon

コモディティハードウェア上のオーバーレイ実装を選択

Amazon VPCが選んだ現実解

データ(MTU)はすべてのサービスで1500バイトを確保
多くのサービスではMTU=9001まで対応



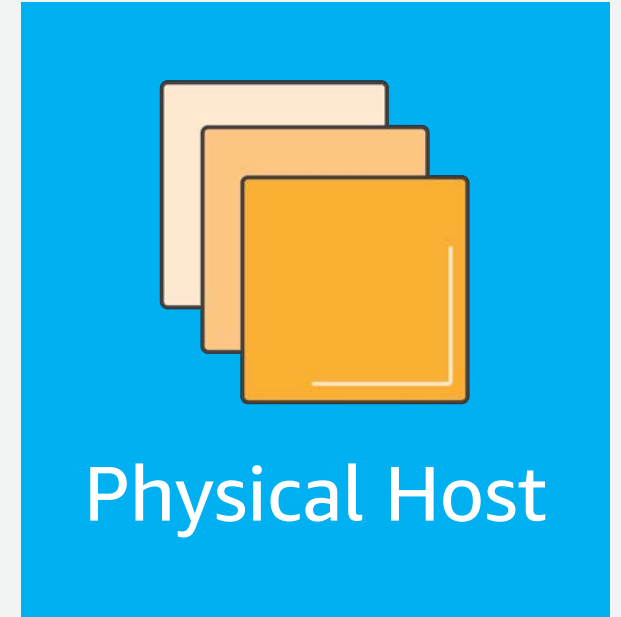
VPCの各種機能に必要な情報を記述

- ✓ リージョン情報
- ✓ VPC-ID
- ✓ セキュリティグループ
- ✓ NACL
- ✓ ピアリング状態
- ✓

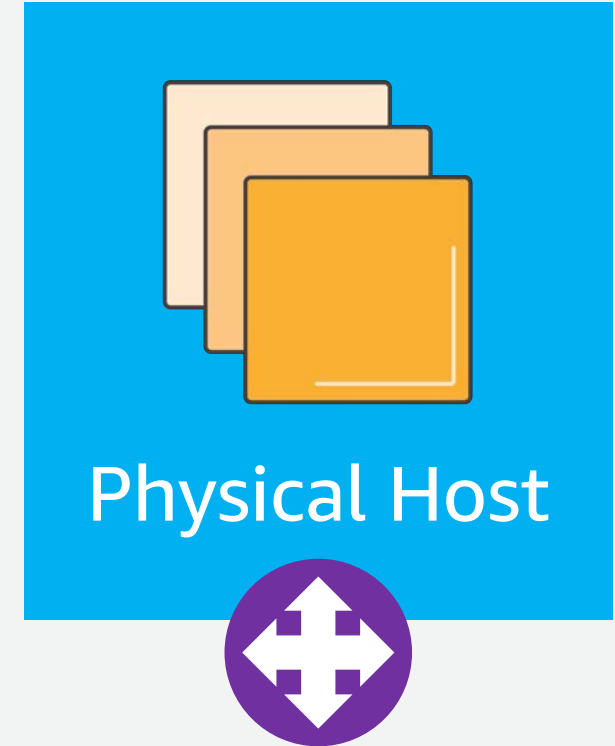
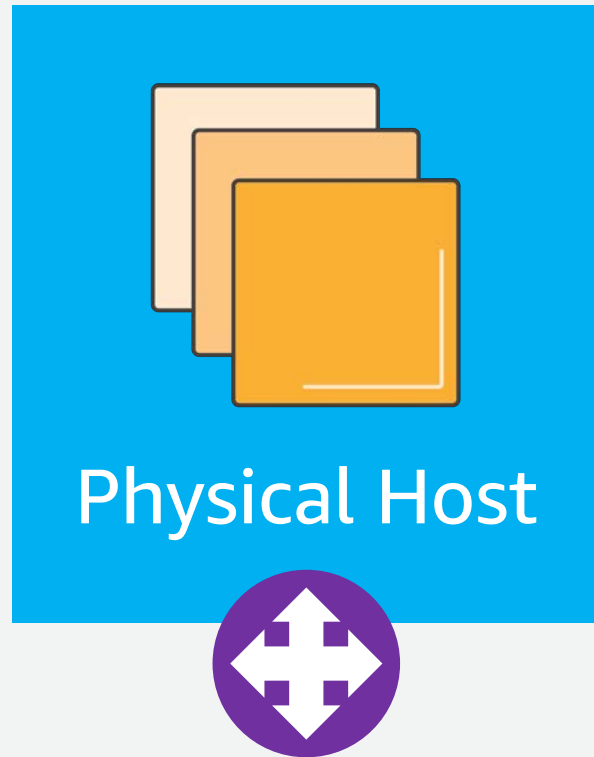
パケットのカプセル化

- 一番外側のIPは物理ホスト宛
- パケットにはVPCとENIがカプセル化される
- マッピングサービスによって送信側はそれらを知る

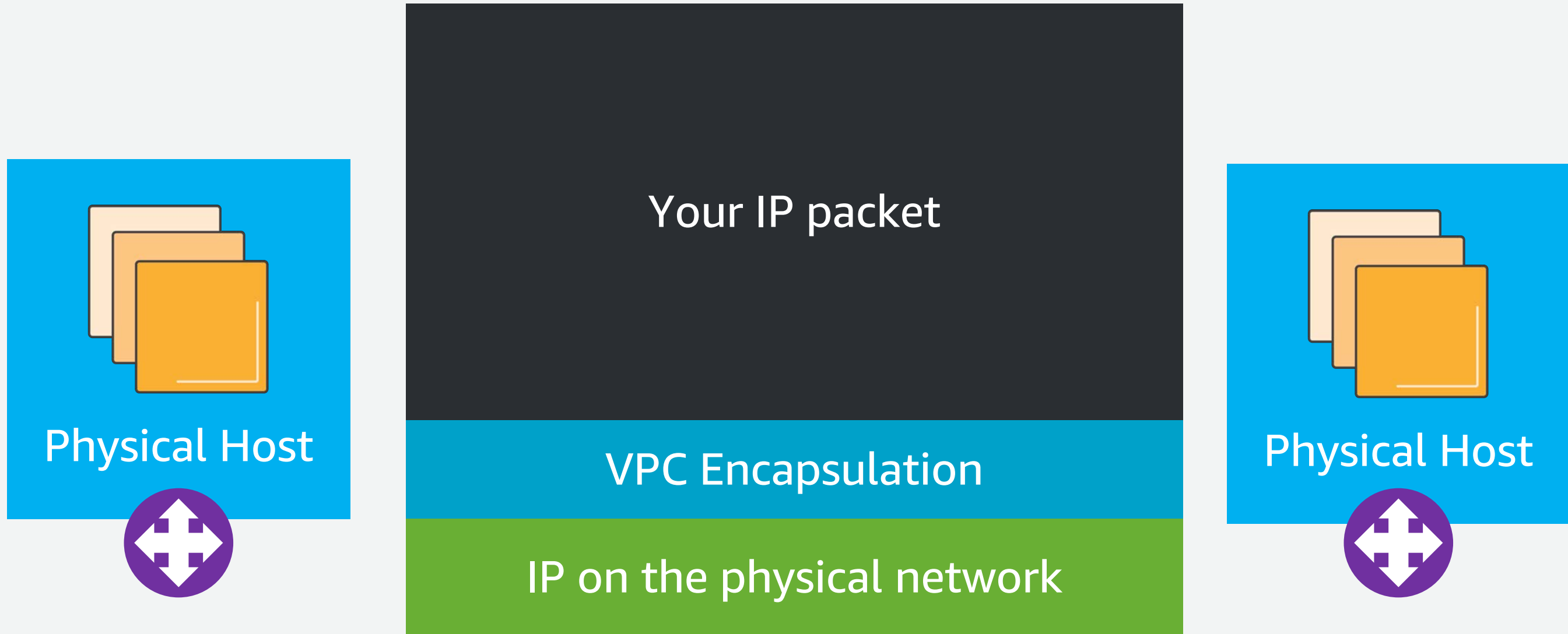
VPCの物理実装



VPCの物理実装

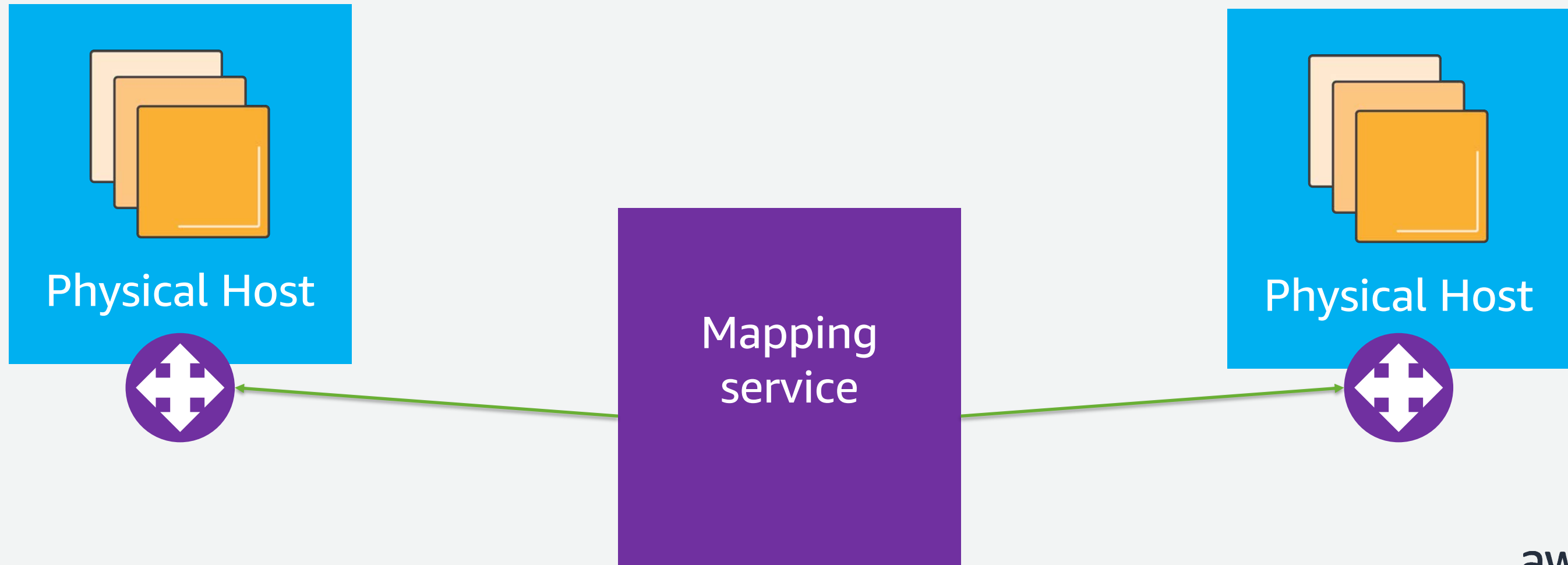


VPCの物理実装



物理と論理の紐付け＝Mapping Service

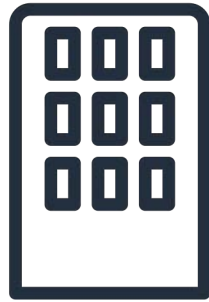
- 送信先となる物理ホスト、IPアドレス、カスタマVPC経路のマッピングを行う分散されたウェブサービス
- マイクロ秒のレイテンシに対応するため、マッピング情報はキャッシュされる。変更時には当然積極的に無効化される。



The mapping service

- 送信先となる物理ホスト、IPアドレス、カスタマVPC経路のマッピングを行う分散されたウェブサービス
- マイクロ秒のレイテンシに対応するため、マッピング情報はキャッシュされる。変更時には当然積極的に無効化される。

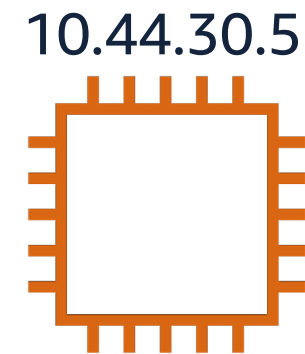
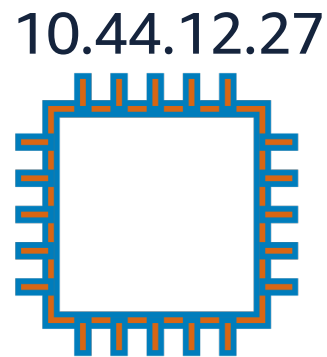
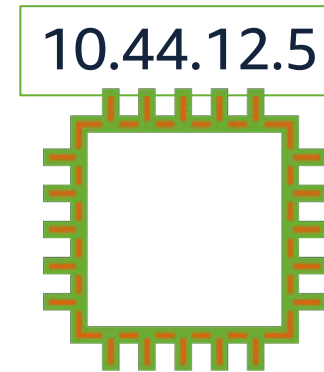
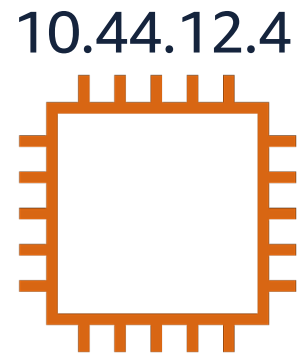
EC2 Classicの限界



Corporate data center
192.168.0.0/16



- 192.168.0.0/16: local
- 10.44.12.4/32: AWS
- 10.44.30.5/32: AWS
- 10.44.12.5/32: AWS
- 10.44.12.27/32: AWS



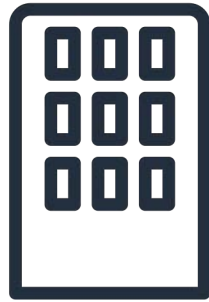
カスタマの必要としてるもの

自分の好きなIPアドレス

経路集約

既存のネットワークとの適合

Virtual Private Cloud



VPN
Connection



Corporate data
center
192.168.0.0/16



192.168.0.0/16: local

172.16.0.0/16: AWS

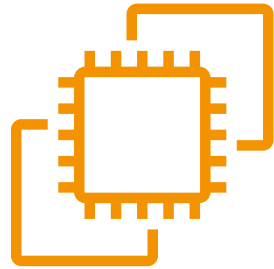
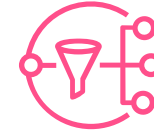
172.16.10.0/24

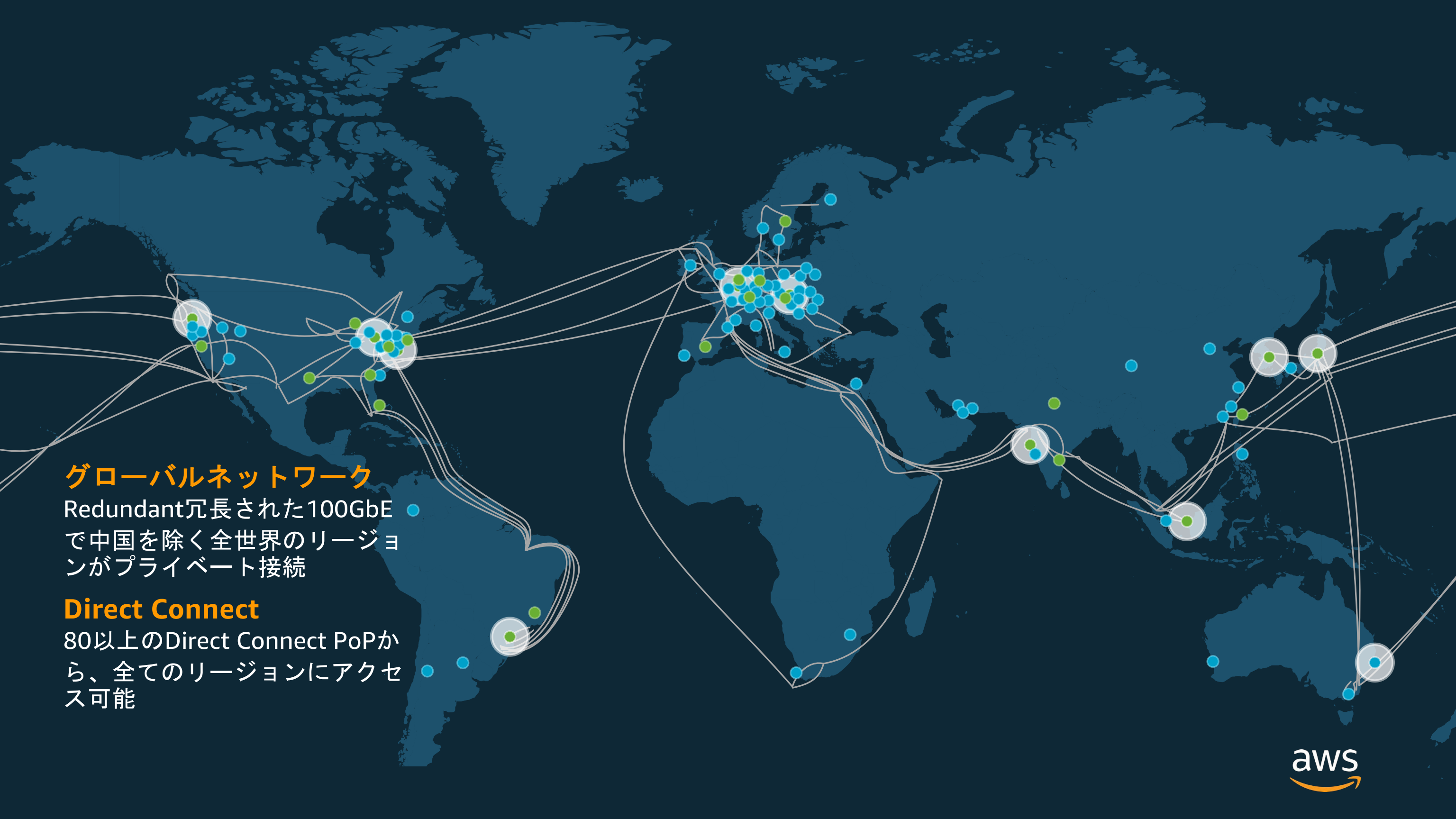
172.16.20.0/24

Internet
gateway



今日のVPC





グローバルネットワーク

Redundant冗長された100GbE
で中国を除く全世界のリージョン
がプライベート接続

Direct Connect

80以上のDirect Connect PoPから、
全てのリージョンにアクセス可能

インターネットとの接続

Interconnection facilities/carrier hotels

Internet exchanges

The screenshot shows the PeeringDB website interface. At the top, there is a search bar with the text "Search here for a network, IX, or facility." and a "Register or Login" button. Below the search bar, the "Amazon.com" entry is highlighted as a "Diamond Sponsor".

Amazon.com Details:

Organization	Amazon.com
Also Known As	Amazon Web Services
Company Website	http://www.amazon.com
Primary ASN	16509
IRR Record	AS-AMAZON
Route Server URL	
Looking Glass URL	
Network Type	Enterprise
IPv4 Prefixes	4000
IPv6 Prefixes	1500
Traffic Levels	Not Disclosed
Traffic Ratios	Balanced
Geographic Scope	Global
Protocols Supported	<input checked="" type="radio"/> Unicast IPv4 <input type="radio"/> Multicast <input checked="" type="radio"/> IPv6
Last Updated	2018-05-28T11:08:01Z
Notes	<p>If you have a connectivity issue to Amazon then please visit: IPv4: http://ec2-reachability.amazonaws.com/ IPv6: http://ipv6.ec2-reachability.amazonaws.com/</p> <p>And include detail on prefixes you think you have a problem with if you contact our Ops alias. This will reduce time with troubleshooting.</p> <p>The following Amazon US locations and associated IX's carry routes/traffic specific only to the services with infrastructure in that metro. For example, Jacksonville is CloudFront only, whereas Ashburn is CloudFront, EC2, S3, etc.) - Seattle - Palo Alto - San Jose - Los Angeles - Dallas - St Louis - South Bend - Jacksonville - Miami - Ashburn - Vienna - Newark - New York</p> <p>The following locations and associated IX's are part of Amazon's European Backbone, carrying routes/traffic for</p>

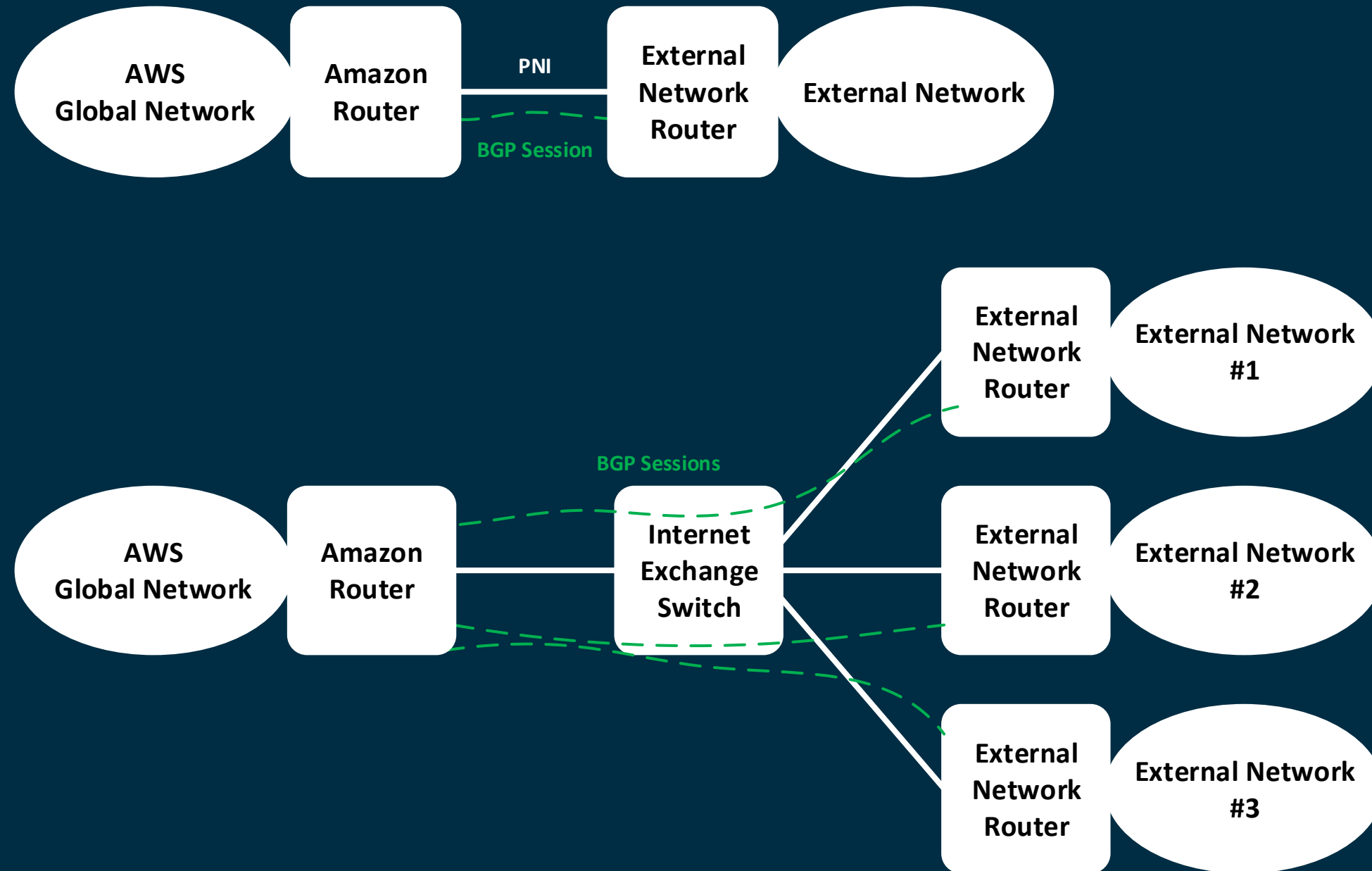
Public Peering Exchange Points:

Exchange	ASN	IPv4	IPv6	Speed
AMS-IX	16509	80.249.210.100	2001:7f8:1::a501:6509:1	400G
AMS-IX	16509	80.249.210.217	2001:7f8:1::a501:6509:2	400G
AMS-IX Chicago	16509	206.108.115.36	2001:504:38:1:0:a501:6509:1	40G
AMS-IX Hong Kong	16509	103.247.139.10	2001:df0:296::a501:6509:1	10G
BBIX Osaka	16509	218.100.9.24	2001:de8:c:2:0:1:6509:1	100G
BBIX Tokyo	16509	218.100.6.52	2001:de8:c::1:6509:1	200G
BBIX Tokyo	16509	218.100.6.207	2001:de8:c::1:6509:2	200G
BCIX	16509	193.178.185.95	2001:7f8:19:1::407d:1	200G
Boston Internet Exchange	16509	206.108.236.70	2001:504:24:1::407d:1	20G
Boston Internet Exchange	16509	206.108.236.80	2001:504:24:1::407d:2	20G
CoreSite - Any2 California	16509	206.72.210.146	2001:504:13::146	30G
CoreSite - Any2 California	16509	206.72.211.146	2001:504:13::211:146	30G
DE-CIX Dallas	16509	206.53.202.25	2001:504:61::407d:0:1	20G
DE-CIX Frankfurt	16509	80.81.194.152	2001:7f8::407d:0:1	400G

Private Peering Facilities:

Facility	ASN	Country	City
151 Front Street West Toronto	16509	Canada	Toronto
35 John Street / 250 Front Street West	16509	Canada	Toronto

PNIs & internet exchanges



BGP messages

